Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko

Doktorska disertacija

PROTOKOL ZA OVERJANJE IN DOGOVOR O KLJUČU ZA UPORABO V BREZŽIČNIH TELESNIH SENZORSKIH OMREŽJIH

Maribor, april 2019 Marko Kompara

Univerza v Mariboru

Fakulteta za elektrotehniko,
računalništvo in informatiko

Doktorska disertacija

PROTOKOL ZA OVERJANJE IN DOGOVOR O KLJUČU ZA UPORABO V BREZŽIČNIH TELESNIH SENZORSKIH OMREŽJIH

Maribor, april 2019

Marko Kompara

Mentor: doc. dr. Marko Hölbl

UDK: 004.057.4:004.7.056.5(043.3)

PROTOKOL ZA OVERJANJE IN DOGOVOR O KLJUČU ZA UPORABO V BREZŽIČNIH TELESNIH SENZORSKIH OMREŽJIH

Doktorska disertacija

Avtor:	Marko Kompara
Mentor:	doc. dr. Marko Hölbl

Naslov:	Protokol za overjanje in dogovor o ključu za uporabo v brezžičnih telesnih senzorskih omrežjih
Naslov v angleščini:	Authentication and Key Agreement Protocol for Wireless Body Sensor Network
UDK:	004.057.4:004.7.056.5(043.3)
Ključne besede:	overjanje, vzpostavitev ključa, dogovor o ključu, telesno senzorsko omrežje, varnostni protokol
Lektoriranje:	izr. prof. dr. Darinka Verdonik
Število izvodov:	
Kraj in datum:	Maribor, april 2019

ZAHVALA

Najprej se zahvaljujem mentorju doc. dr. Marku Hölblu za povabilo k sodelovanju, za usmeritev v študiju in za odgovore na vsa vprašanja, tudi tista bolj "neumna". Prav tako se zahvaljujem vsem članom LPT za pomoč, spodbudo in "razumevanje".

Za financiranje študija se zahvaljujem Javni agenciji za raziskovalno dejavnost Republike Slovenije.

Posebej bi se rad zahvalil staršem, ki so mi omogočili študij in me pri njem vedno podpirali.

Nazadnje pa še hvala vsem ostalim, ki so kakor koli pripomogli h kakovosti mojega študija.

Protokol za overjanje in dogovor o ključu za uporabo v brezžičnih telesnih senzorskih omrežjih

Ključne besede: overjanje, vzpostavitev ključa, dogovor o ključu, telesno senzorsko omrežje, varnostni protokol

UDK: 004.057.4:004.7.056.5(043.3)

Povzetek

Napredek na področjih mikroelektronike, vgrajenega računalništva in brezžične komunikacije je povzročil povečanje zanimanja za telesna senzorska omrežja. Telesno senzorsko omrežje sestavljajo senzorska vozlišča, porazdeljena v neposredni bližini telesa uporabnika, na telesu ali celo v telesu uporabnika. Vozlišča zbirajo fiziološke in druge podatke o stanju telesa in jih posredujejo zmogljivejšim napravam v obdelavo. Takšna oblika omrežja predstavlja predvsem potencial v razvoju in zmanjševanju stroškov zdravstvene oskrbe. Podatki, ki se pretakajo v takšnih omrežjih, so občutljivi. Zdravstveni podatki so tudi zakonsko opredeljeni kot posebna oblika osebnih podatkov, za katere je nujna dodatna skrbnost pri njihovem varovanju. Poleg varnega hranjenja takšnih podatkov je treba zagotavljati njihovo varnost tudi med prenosom iz senzorskih naprav v druge naprave v omrežju. To varovanje je v veliki meri odvisno od protokola overjanja in vzpostavitve ključa, ki preveri istovetnost naprav v komunikaciji in vzpostavi ključ, na podlagi katerega bo nadaljnja komunikacija šifrirana. Razvoj protokola za overjanje in vzpostavitev ključa, primernega za uporabo v telesnih senzorskih omrežjih, je zaradi zahtevane ravni varovanja in strojnih omejitev velik izziv. Cilj te disertacije je razvoj lastnega protokola za overjanje in dogovor o ključu, ki bo izpolnjeval vse varnostne zahteve in bo obenem učinkovit ter primeren za uporabo v senzorskih vozliščih. V ta namen so v doktorski disertaciji zbrane varnostne lastnosti, ki bi jih varni protokoli, primerni za uporabo v telesnih senzorskih omrežjih, morali izpolnjevati, ter možni napadi, na katere bi morali biti odporni. V okviru doktorske disertacije je bil izveden pregled literature, na podlagi katere je bila razvita nova klasifikacija obstoječih protokolov vzpostavitve ključa. Ob pregledu obstoječih protokolov je bila posebna pozornost posvečena tudi analizam, ki so jih avtorji takšnih protokolov izvedli za dokazovanje varnosti in učinkovitosti predstavljenih protokolov. Iz tega je nastal seznam metod vrednotenja varnosti in učinkovitosti protokolov. Disertacija predstavi dva nova lahka protokola vzpostavitve ključa, namenjena uporabi v telesnih senzorskih omrežjih. Protokola omogočata vzpostavitev komunikacije s senzorskim vozliščem na varen in nezahteven način. V dokaz tega je za vsak protokol opravljena varnostna analiza s hevristično metodo vrednotenja varnosti in analiza učinkovitosti, ki vključuje tudi primerjavo predlaganih protokolov z obstoječimi sorodnimi protokoli.

Authentication and Key Agreement Protocol for Wireless Body Sensor Network

Key words: authentication, key establishment, key agreement, body sensor network, security protocol

UDC: 004.057.4:004.7.056.5(043.3)

Abstract

Advances in the fields of microelectronics, embedded computing, and wireless communications have caused the interest in wireless body sensor networks to rise sharply. A body sensor network is constructed from sensor nodes distributed in direct vicinity, on, and even in the user's body. The nodes collect physiological and other data about the state of the body and forward them on to more powerful devices for processing. This sort of network has wide application potential in the development and cost reduction of healthcare. Devices in such networks collect highly sensitive data. Health data is also legally recognised as a special form of personal data that require particular diligence in their protection. In addition to safely storing such data, it is also necessary to ensure their safety during transmission from sensor devices to other devices in the network. This security is highly dependent on the authentication and key establishment protocol, which verifies the identity of the devices in communication and establishes the key, with which all further communication will be encrypted. Development of a new authentication and key establishment protocol for body sensor network is a major challenge due to the required level of security and severe hardware constraints. The goal of this dissertation is the development of our own protocol for authentication and key agreement that meets all the security requirements and is also efficient and suitable for use on sensor nodes. For this purpose, the doctoral dissertation catalogues security requirements and possible attacks, which a secure protocol suitable for use in body sensor network should meet and be resistant to. A review of relevant literature was conducted, on basis of which a new classification of existing key establishment protocols was developed. When reviewing the existing protocols, special attention was paid to the analyses carried out by the authors to prove the security and effectiveness of the presented protocols. Based on this a list of all the methods for evaluating the security and effectiveness of protocols was created. The dissertation presents two new lightweight authentication and key establishment protocols for use in body sensor networks. The protocols provide a safe and efficient way to establish communication with the sensor nodes. To prove this, security analyses has been performed using an ad hoc security evaluation method, as well as efficiency analyses that include a comparison of the proposed protocols with existing similar protocols.

Kazalo

1 UVOD 1

1.1 Opredelitev problema 1

1.2 Cilji doktorske disertacije 3

1.3 Teza doktorske disertacije 4

1.4 Predpostavke in omejitve 4

1.5 Pričakovani izvirni znanstveni prispevki 5

1.6 Struktura doktorske disertacije 5

2 TELESNA SENZORSKA OMREŽJA 7

2.1 Internet stvari in brezžična senzorska omrežja 7

2.1.1 Internet stvari 8

2.1.2 Brezžično senzorsko omrežje 9

2.2 Pregled področja brezžičnih telesnih senzorskih omrežij 11

2.2.1 Struktura komunikacije 12

2.2.2 Umestitev TSO med druge vrste omrežij 13

2.2.3 Primerjava telesnih senzorskih omrežij in brezžičnih senzorskih omrežij 14

3 PROTOKOLI ZA OVERJANJE IN DOGOVOR O KLJUČU 17

3.1 Vzpostavitev ključa 17

3.2 Overjanje 19

3.3 Kriptografski gradniki protokolov overjanja in vzpostavitve ključa 20

3.3.1 Osnovni gradniki in operacije 20

3.3.2 Kriptografska zgoščevalna funkcija 22

3.3.3 Simetrična šifra 23

3.3.4 Asimetrična kriptografija 24

4 PROTOKOLI VZPOSTAVITVE KLJUČA V TELESNIH SENZORSKIH OMREŽJIH 28

4.1 Pregled varnostnih zahtev 32

4.2 Pregled napadov na protokole 34

4.3 Klasifikacija protokolov za vzpostavitev ključa v telesnih senzorskih omrežjih 38

4.3.1 Tradicionalni protokoli vzpostavitve ključa 40

4.3.2 Protokoli vzpostavitve ključa na osnovi fizioloških podatkov 42

4.3.3 Protokoli vzpostavitve ključa z generiranjem skrivnega ključa 48

4.3.4 Hibridni protokoli vzpostavitve ključa 52

5 VREDNOTENJE VARNOSTI IN UČINKOVITOSTI PROTOKOLOV ZA VZPOSTAVITEV KLJUČA V TELESNIH SENZORSKIH OMREŽJIH 55

5.1 Metode vrednotenja varnosti protokolov 55

5.1.1 Hevristično vrednotenje varnosti 55

5.1.2 Formalno preverjanje varnosti 58

5.1.3 Delno formalno preverjanje varnosti 58

5.1.4 Preverjanje varnosti v protokolih na osnovi fizioloških podatkov 59

5.1.5 Preverjanje varnosti v protokolih z generiranjem skrivnega ključa 60

5.1.6 Ostale metode preverjanja varnosti 60

5.2 Razprava o vrednotenju varnosti protokolov za vzpostavitev ključa v TSO 60

5.3 Metode vrednotenja učinkovitosti protokolov 61

5.3.1 Učinkovitost porabe pomnilnika 62

5.3.2 Računska zahtevnost 62

5.3.3 Učinkovitost komunikacije 63

5.3.4 Učinkovitost porabe energije 64

5.3.5 Vrednotenje učinkovitosti protokolov vzpostavitve ključa na osnovi fizioloških podatkov 64

5.3.6 Vrednotenje učinkovitosti protokolov vzpostavitve ključa z generiranjem skrivnega ključa 66

5.4 Razprava o vrednotenju učinkovitosti protokolov za vzpostavitev ključa v TSO 66

5.5 Izbor metod za ocenjevanje varnosti in učinkovitosti novo razvitih protokolov 68

6 IZBOLJŠANI PROTOKOL ZA OVERJANJE IN VZPOSTAVITEV KLJUČA V TELESNIH SENZORSKIH OMREŽJIH 70

6.1 Protokol Abdmeziem-Tandjaoui in njegove pomanjkljivosti 71

6.1.1 Analiza delovanja protokola Abdmeziem-Tandjaoui 73

6.2 Izboljšani protokol za overjanje in vzpostavitev ključa v telesnih senzorskih omrežjih 76

6.2.1 Izboljšave novega protokola I 78

6.3 Varnostna analiza protokola I 79

6.4 Analiza učinkovitosti protokola I 82

7 RAZVOJ PROTOKOLA ZA OVERJANJE IN DOGOVOR O KLJUČU ZA UPORABO V BREZŽIČNIH TELESNIH SENZORSKIH OMREŽJIH 89

7.1 Nov protokol za overjanje in dogovor o ključu v telesnih senzorskih omrežjih 91

7.1.1 Faza inicializacije 92

7.1.2 Faza registracije 92

7.1.3 Faza overjanja in dogovora o ključu 92

7.2 Varnostna analiza protokola II 95

7.3 Analiza učinkovitosti protokola II 99

8 ZAKLJUČEK 103

LITERATURA 106

Kazalo slik

Slika 2.1: Povprečen potencial vpeljave IoT v posamezne panoge [28]. 9
Slika 2.2: Struktura komunikacije [56]. 13
Slika 2.3: Umestitev TSO v brezžična omrežja [57, 58]. 14
Slika 3.1: Preprosta klasifikacija tehnik vzpostavitve ključa [59]. 19
Slika 3.2: Postopek simetričnega šifriranja. 23
Slika 3.3: Postopek asimetričnega šifriranja. 24
Slika 4.1: Vzpostavitev ključa s pomočjo mehkega trezorja [132]. 47
Slika 6.1: Izmenjava sporočil v protokolu Abdmeziem-Tandjaoui [122]. 73
Slika 6.2: Izmenjava sporočil v novem protokolu I [205]. 78
Slika 6.3: Odstopanje v oceni porabe električne energije v raziskavi Abdmeziem-Tandjaoui in popravljeni oceni porabe [205]. 84
Slika 7.1: Omrežni model TSO za predlagani protokol overjanja in dogovora o ključu [90]. 90
Slika 7.2: Faza overjanja in dogovora o ključu novega protokola II [212]. 94

Kazalo tabel

Tabela 2.1: Razlike med TSO in brezžičnimi senzorskimi omrežji [51, 53]. 15

Tabela 3.1: Primerjava velikosti ključev simetričnih in asimetričnih šifer ob enakovredni ravni varnosti [66] 25

Tabela 5.1: Seznam protokolov vzpostavitve ključa v TSO in njihove varnostne lastnosti. ... 56

Tabela 6.1: Definicija okrajšav, uporabljenih v poglavju 6. 70

Tabela 6.2: Definicija simbolov, uporabljenih v analizi učinkovitosti. 85

Tabela 6.3: Seznam računskih operacij, ki jih opravi senzorsko vozlišče v protokolu Abdmeziem-Tandjaoui in novem protokolu I. 86

Tabela 6.4: Ocena porabe električne energije senzorskega vozlišča v računskih operacijah protokola Abdmeziem-Tandjaoui in novega protokola I. 86

Tabela 6.5: Seznam poslanih in prejetih vrednosti senzorskega vozlišča v protokolu Abdmeziem-Tandjaoui in novem protokolu I. 87

Tabela 6.6: Stroški komunikacije senzorskega vozlišča v protokolu Abdmeziem-Tandjaoui in novem protokolu I. 88

Tabela 7.1: Definicija okrajšav, uporabljenih v poglavju 7. 91

Tabela 7.2: Primerjava porabe trajnega pomnilnika in računske zahtevnosti novega protokola II s sorodnimi protokoli. 101

Tabela 7.3: Primerjava časovne zahtevnosti računskih operacij in porabe električne energije novega protokola II s sorodnima protokoloma na 32-bitnem mikrokrmilniku Cortex-M3. 101

Tabela 7.4: Primerjava učinkovitosti komunikacije novega protokola II s sorodnimi protokoli. 102

Seznam uporabljenih kratic in simbolov

AES	Advanced Encryption Standard
AVISPA	Automated Validation of Internet Security Protocols and Applications
BAN	Body Area Network
BAN logic	Burrows–Abadi–Needham logic
BANT	Body Area Network for Telemedicine
BASN	Body Area Sensor Network
BSN	Body Sensor Network
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CMAC	Cipher-based Message Authentication Code
CTR	Counter mode
DES	Data Encryption Standard
DoS	Denial of Service
ECC	Eliptic Curve Cryptography
ECG	Electrocardiogram
EEG	Elektroencefalogram
EKG	Elektrokardiogram
EMG	Elektromiogram
FAR	False Acceptance Rate
FPG	Fotopletizmogram
FRR	False Rejection Rate
GCM	Galois/Counter Mode
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HMAC	Hash-Based Message Authentication Code
HTER	Half Total Error Rate
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers

IMD	Implantable Medical Device
IoT	Internet of Things
IPI	Interpulse Interval
KEK	Kriptografija Eliptičnih Krivulj
km	Kilometer
LTE	Long-Term Evolution
m	Meter
M2M	Machine to machine
MAC	Message Authentication Code
MEMS	Micro-Electro-Mechanical Systems
MD5	Message-Digest algorithm 5
MiTM	Man in The Middle Attack
NIST	National Institute of Standards and Technology
OCB	Offset Codebook Mode
PAN	Personal Area Network
PKI	Public Key Infrastructure
PPG	Photoplethysmogram
RC4	Rivest Cipher 4
RSA	Rivest–Shamir–Adleman
RSSI	Received Signal Strength Indicator
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
SHA-3	Secure Hash Algorithm 3
TMIS	Telecare Medicine Information System
TSO	Telesno Senzorsko Omrežje
UMTS	Universal Mobile Telecommunications System
WBAN	Wireless Body Area Network
WBASN	Wireless Body Area Sensor Network
WBSN	Wireless Body Sensor Network
WHMS	Wearable Health-Monitoring Systems
WiMAX	Worldwide Interoperability for Microwave Access

WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMSN	Wireless Medical Sensor Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network
XOR	Ekskluzivni ali ali izključujoči ali

1 Uvod

1.1 Opredelitev problema

Zaupnost komunikacije je že od nekdaj zelo pomembna. Najstarejši zapisi, ki vsebujejo zakrivanje njihovega pomena, segajo v obdobje 1900 let pred našim štetjem [1]. Po začetku uporabe računalnikov za namene kriptografije je ta še vedno ostala v domeni državnih organizacij. Kriptografija se je prebila v javno domeno s predstavitvijo javnega šifrirnega standarda DES (Data Encryption Standard) in kriptografije javnega ključa [2–4]. V desetletjih, ki so sledila, sta se zmogljivost in uporaba osebnih računalnikov močno povečali [5]. Temu so sledili tudi protokoli za zagotavljanje zaupnosti. Kmalu se je pojavila ideja za internet stvari (angl. Internet of Things – IoT) [4]. To so vseprisotne naprave z vgrajeno elektroniko, programsko opremo in sposobnostjo povezovanja. Ker takšne naprave tipično pošiljajo podatke preko javnega omrežja (internet) in ker pošiljajo podatke o stanju v njihovem okolju, ki so potencialno zasebne narave, je zaupnost v takšnih omrežjih pomembna. IoT sestavljajo pretežno naprave z omejeno zmogljivostjo (tipično gre za majhne naprave). Omenjene omejitve so posebej poudarjene v podskupini IoT-omrežij, imenovani Telesna Senzorska Omrežja – TSO (angl. Body Area Network – BAN ali Body Sensor Network – BSN). Naprave v takšnih omrežjih zbirajo in posredujejo zasebne podatke o fiziološkem stanju uporabnika. Zaradi okolja, v katerem se nahajajo, so senzorske naprave skrajno fizično omejene. Posledica majhne velikosti je tudi omejena zmogljivost naprav. Moderni protokoli za zagotavljanje varne komunikacije so tipično neprimerni za takšna okolja, saj niso zgrajeni za delovanje v tako omejenih okoljih [6]. Pri tem mislimo predvsem na kriptografijo javnega ključa, ki se sicer primarno uporablja v procesu overjanja in vzpostavitve ključa (angl. authentication and key establishment).

Prvo telesno senzorsko omrežje je predstavil T.G. Zimmerman leta 1996 kot posebno obliko osebnega omrežja (angl. Personal Area Network – PAN) [7]. Danes se TSO uvrščajo med brezžična senzorska omrežja (Wireless Sensor Network – WSN), s katerimi imajo tudi marsikaj skupnega. Telesna senzorska omrežja so definirana v IEEE 802.15 kot komunikacijski standard za nizkozmogljive naprave, ki so locirane v telesu, na telesu ali v bližini (človeškega) telesa in delujejo v korist uporabnika [8]. Napredek na področjih mikroelektronike, vgrajenega računalništva in brezžičnih komunikacij je omogočil razvoj in implementacijo takšnih omrežij ter povečal zanimanje za to tehnologijo. Ob staranju svetovne populacije [9], večanju števila kroničnih bolnikov [10] in velikem finančnem bremenu, ki ga predstavlja zdravstvo, je zanimanje za razvoj novih rešitev, ki bi zmanjšale breme zdravstvene nege in bi bile ob tem nevsiljive za uporabnika, zanesljive ter istočasno tudi cenovno ugodne, zelo veliko. TSO je tehnologija, ki omogoča vse to.

TSO je sestavljeno iz več biosenzorjev z omejeno zmogljivostjo, ki merijo različne fiziološke signale, ki jih proizvaja telo in zunanje signale o stanju telesa oziroma uporabnika (npr. pospešek) [8, 11]. Senzorji in druge naprave v omrežju prejemajo in pošiljajo podatke preko brezžične povezave z nizko porabo energije [12]. Senzorji, ki sestavljajo TSO so lahko vgrajeni v telo, se nosijo na površini telesa v obliki obliža ali so integrirani v uporabnikova oblačila. Naprave, ki so vgrajene v telo, se pogosto poimenujejo medicinski pripomočki za vsaditev (angl. Implantable Medical Device – IMD). TSO predstavljajo velik potencial za bodoč razvoj zdravstvene nege. Alternativni primeri uporabe TSO so še na bojiščih za namene nadzora stanja vojakov, na področju športa in v razvedrilne namene. TSO pošiljajo fiziološke podatke, iz katerih je mogoče razbrati zdravstveno stanje uporabnika. Poleg tega je iz komunikacije mogoče razbrati še veliko drugega o življenju uporabnika (aktivnost, navade, ipd.). Zakon o varstvu osebnih podatkov (ZVOP-1) [13], ki velja v Sloveniji, in splošna uredba o varstvu podatkov (angl. General Data Protection Regulation – GDPR) [14], ki velja v Evropski uniji, uvrščata podatke o zdravstvenem stanju med občutljive oziroma posebno vrsto osebnih podatkov. To nam da vedeti, da gre za zelo občutljive podatke, in temu je treba prilagoditi tudi raven njihove zaščite. Pomemben del te zaščite je tudi varovanje zaupnosti podatkov med prenosom. Kakovost zaščite podatkov pri prenosu je v veliki meri odvisna od uporabljenega protokola za vzpostavitev ključa. Dodatne zahteve pri razvoju protokola za overjanje in vzpostavitev ključa, ki je primeren za uporabo v TSO, predstavljajo še energijska učinkovitost in strojne omejitve, ki so prisotne predvsem na senzorskih vozliščih, ter zanesljivost delovanja, ki je zahtevana v zdravstvenih sistemih.

Fokus te disertacije je zagotavljanje varne komunikacije senzorskih naprav z zmogljivejšimi napravami, kjer je učinkovitost uporabljenih protokolov zelo pomembna. Komunikacija zunaj tega področja se izvaja med napravami, ki nimajo zmogljivostnih omejitev, ki bi preprečevale uporabo sodobnih protokolov za vzpostavitev ključa. Omejitve senzorskih naprav so posledica fizičnih omejitev (velikosti) samih naprav, okolja, v katerem se nahajajo in delujejo, ter kot posledica podatkov, ki jih obdelujejo. Omejitve naprav se prenesejo v izzive, ki so prisotni pri zasnovi protokola za overjanje in vzpostavitev ključa. Glavni izzivi so dolgotrajno delovanje ob upoštevanju omejene zaloge energije, omejeni računski in pomnilniški viri ter potrebna visoka raven varovanja.

Podatki se v TSO pošiljajo po brezžičnih povezavah, zato jih je treba zavarovati pred prisluškovalci in pred spremembami. Da to dosežemo, je treba uporabiti šifrirni algoritem, ki pa za svoje delovanje potrebuje skrivni ključ. Zato je treba imeti dodaten protokol, ki na primeren način ustvari ključ in ga na varen način dostavi deležnikom v komunikaciji. Takšen proces imenujemo vzpostavitev ključa. Vzpostavitev ključa je proces, ki omogoča dvema ali več deležnikom varno izmenjavo ključev. Dogovor o ključu je posebna oblika vzpostavitve ključa. Overjanje je ločena funkcionalnost, ki pa se tipično opravi hkrati oziroma tik pred vzpostavitvijo ključa ali po njej. Overjanje preveri istovetnost deležnikov v komunikaciji in prepreči, da bi se ključ dodelil tretji osebi, ki nima dovoljenja za sodelovanje v komunikaciji oziroma ni del omrežja. Overjanje in vzpostavitev ključa je prvi in najpomembnejši korak za

zagotavljanje zaupnosti, avtentičnosti in celovitosti, ki jo naprave, ki želijo varno komunicirati, opravijo.

Izziv protokolov za overjanje in vzpostavitev ključa v TSO je zadostiti naboru zahtev, ki je širši (v zahtevah učinkovitosti delovanja) kot za splošne protokole overjanja in vzpostavitve ključa. To je tudi razlog, zakaj obstoječe rešitve niso primerne za uporabo v tem okolju. Protokoli za overjanje in vzpostavitev ključa, primerni za delovanje v TSO, morajo biti odporni na odtujitev naprav, prilagodljivi sestavi omrežja, varčni in učinkoviti z izrabo virov.

V doktorski disertaciji bo obravnavano področje varovanja komunikacije, in sicer bomo govorili o protokolih za overjanje in vzpostavitev ključa, ki so prilagojeni delovanju v telesnih senzorskih omrežjih. Takšen protokol mora biti robusten, učinkovit ter predvsem varen. Omogočati mora zasebnost komunikacije, overjanje vseh vpletenih entitet in preprečevati možnost korelacije med sporočili in specifičnim uporabnikom. V literaturi obstaja že precej protokolov za vzpostavitev ključa, ki so namenjeni uporabi v TSO. Končni cilj te doktorske disertacije je razviti nov lahek protokol, prilagojen za uporabo v TSO s tradicionalnim delovanjem, ki bo omogočal overjanje in odgovor o ključu ter bo varnejši in/ali učinkovitejši od primerljivih predhodnih protokolov.

1.2 Cilji doktorske disertacije

Na podlagi opredeljenega problema bomo v doktorski disertaciji želeli doseči sledeče cilje in ustvariti novost na raziskovalnem področju overjanja in vzpostavitve ključa v TSO:

- na podlagi pregleda obstoječih protokolov za overjanje in vzpostavitev ključa v TSO ustvariti novo klasifikacijo protokolov, tako da bo iz tipa protokola mogoče razbrati, katere vhodne podatke oziroma metode protokol uporablja za varno vzpostavitev ključa,
- izvesti identifikacijo uporabe različnih metod za preverjanje varnostnih lastnosti in odpornosti na napade v novo predlaganih protokolih za vzpostavitev ključa,
- izvesti identifikacijo uporabe različnih metod merjenja učinkovitosti v novo predlaganih protokolih za vzpostavitev ključa,
- razvoj novega lahkega protokola za overjanje in dogovor o ključu, primernem za uporabo v TSO med senzorskimi napravami in zmogljivejšo napravo, ki nato posreduje zbrane podatke zdravstvenim ustanovam,
- z najpogostejšo metodo preverjanja varnosti protokola in najpogosteje uporabljeno metodo merjenja učinkovitosti protokola, kot smo jih določili pri izpolnjevanju prejšnjih ciljev, pokazati, da je nov protokol bolj varen in/ali bolj učinkovit od drugih primerljivih protokolov za overjanje in vzpostavitev ključa, ki so namenjeni za delovanje v TSO.

1.3 Teza doktorske disertacije

V nalogi postavimo naslednjo tezo:

Razviti je mogoče nov lahek protokol za overjanje in dogovor o ključu, namenjen uporabi v TSO, ki bo varnejši in/ali učinkovitejši od primerljivih protokolov, pri čemer bo primerjava izvedena glede na najpogosteje uporabljene metode ocenjevanja varnosti in učinkovitosti takšnih protokolov v literaturi.

Na podlagi teze oblikujemo naslednje hipoteze:

Hipoteza 1:

Obstajajo ključne razlike v strukturi in lastnostih obstoječih protokolov za vzpostavitev ključa v TSO, na podlagi katerih je mogoče takšne protokole klasificirati v različne skupine.

Hipoteza 2:

S pomočjo rezultatov prve hipoteze je mogoče razviti nov protokol za overjanje in dogovor o ključu, ki je primeren za delovanje v TSO. Novi protokol zagotavlja varno delovanje glede na podane kriterije iz literature in je odporen na znane napade ter je učinkovit.

1.4 Predpostavke in omejitve

V doktorski disertaciji se bomo omejili na naslednje postavke:

- V raziskavah se bomo omejili na protokole za overjanje in vzpostavitev ključa, ki so namenjeni delovanju v notranjem TSO.
- V raziskavah se bomo omejili na protokole za overjanje in vzpostavitev ključa, ki so namenjeni delovanju preko brezžičnega omrežja.
- V raziskavah se bomo omejili na protokole za overjanje in vzpostavitev ključa, ki ne omejujejo, kje in kako lahko TSO deluje.
- Pri dokazovanju in primerjavi varnosti protokolov se bomo omejili na najpogosteje uporabljen pristop dokazovanja varnosti, ki ga bomo zasledili v literaturi.
- Pri merjenju in primerjavi učinkovitosti protokolov se bomo omejili na uporabo najpogosteje uporabljenih metod v literaturi.
- Primerjavo razvitih protokolov bomo izvedli glede na druge lahke protokole za overjanje in vzpostavitev ključa, namenjene delovanju v TSO.

Istočasno bomo naslednje predpostavke šteli za resnične:

- Predpostavljamo, da osnovni kriptografski gradniki (angl. cryptographic primitive), kot so kriptografska zgoščevalna funkcija (angl. cryptographic hash function), simetrično šifriranje (angl. symmetric encryption) in asimetrično šifriranje (angl. asymmetric encryption), izpolnjujejo vse definirane lastnosti in zahteve takšnih gradnikov.

- Predpostavljamo, da je do naprav, ki bodo vključene v omrežje, mogoče vzpostaviti skrivni kanal (angl. secret channel), prek katerega ni mogoče prisluškovanje ali kakršnokoli poseganje v komunikacijo.
- Predpostavljamo model nasprotnika (angl. Adversary model) z napadalcem, ki ima najboljše možne pogoje za izvedbo napada. To vključuje računsko moč, odtujitev oziroma dostop do naprav, ki se ne nahajajo v varovanem območju, sposobnost prisluškovanja javnim komunikacijskim kanalom, prestrezanja in spreminjanja sporočil na javnem kanalu ter podrobno poznavanje delovanja napadenega protokola.
- Predpostavljamo možnost generiranja naključne enkratne vrednosti (angl. nonce) na nizkozmogljivih napravah.
- Predpostavljamo, da so obstoječi primerljivi protokoli za overjanje in dogovor o ključu za TSO najučinkovitejše in najvarnejše rešitve glede na naravo omrežja in omejitve gradnikov.
- Predpostavljamo, da je določen protokol učinkovitejši, če zahteva manjše število računskih operacij, zasede manj pomnilnika in/ali ima manjšo povprečno časovno zahtevnost.

1.5 Pričakovani izvirni znanstveni prispevki

Predstavljeno tematiko oziroma raziskovalne rezultate bomo razdelili v naslednje predvidene izvirne znanstvene prispevke:

- Izčrpen pregled protokolov za vzpostavitev ključa v TSO, na podlagi katerega bo ustvarjena nova klasifikacija takšnih protokolov. Na podlagi pregleda bo sestavljen nabor vseh napadov na protokole za vzpostavitev ključa v TSO in varnostnih lastnosti, ki jih morajo izpolnjevati. Na podlagi zbranih protokolov oziroma publikacij bo opravljena tudi analiza uporabljenih metod za preverjanje varnosti in učinkovitosti novopredstavljenih protokolov.
- Izdelava varnega protokola za vzpostavitev ključa, namenjenega za uporabo v TSO. Analiza varnosti in učinkovitosti novega protokola z najpopularnejšimi metodami na področju (kot je bo opredeljeno na podlagi prejšnjega prispevka) ter primerjava s predhodnim protokolom.
- Izdelava robustnega in učinkovitega protokola za medsebojno overjanje in dogovor o ključu z nesledljivostjo za uporabo v TSO. Analiza varnosti in učinkovitosti novega protokola z najpogosteje uporabljenimi metodami ter primerjava njegove učinkovitosti z drugimi primerljivimi protokoli.

1.6 Struktura doktorske disertacije

Disertacija je sestavljena iz osmih poglavij. V prvem poglavju je opredeljena problematika, ki je naslovljena v disertaciji skupaj s cilji, tezami, predpostavkami ter omejitvami opravljene

raziskave. Drugo poglavje je namenjeno predstavitvi širšega področja interneta stvari in področja telesnih senzorskih omrežij. Telesna senzorska omrežja so podrobneje opisana in umeščena v spekter različnih omrežij. Naštete so tudi vse specifične lastnosti tega omrežja ter njegove razlike v razmerju do sorodnega brezžičnega senzorskega omrežja. Tretje poglavje opisuje osnovne koncepte protokolov overjanja in vzpostavitve ključa, vključno z glavnimi kriptografskimi gradniki, ki se v takšnih protokolih uporabljajo. Četrto poglavje se začne s predstavitvijo varnostnih lastnosti in možnih napadov, ki jih morajo protokoli za overjanje in vzpostavitev ključa v TSO izpolnjevati oziroma biti nanje odporni. Poglavje se zaključi s pregledom obstoječih protokolov in predlogom nove klasifikacije protokolov za overjanje in vzpostavitev ključa v TSO na podlagi lastnosti protokolov, zajetih v pregledu znanstvene literature. Peto poglavje nadaljuje pregled obstoječih protokolov, vendar se v tem poglavju pozornost posveča metodam analize varnosti in učinkovitosti najdenih protokolov. Šesto poglavje predstavi prvi novi protokol vzpostavitve ključa, primeren za uporabo v TSO. Protokol je izboljšava protokola, najdenega med pregledom literature. Novi protokol ima izboljšano varnost in primerljivo učinkovitost delovanja z izvornim protokolom. Sedmo poglavje predstavi drugi novi protokol. Gre za lahek protokol za overjanje in dogovor o ključu. Za protokol sta izdelani tudi analizi varnosti in učinkovitosti. Protokol je primerjan s podobnimi protokoli, ki smo jih zasledili med pregledom literature. Osmo poglavje povzame in ovrednoti raziskavo, izvedeno v disertaciji, ter poda njene zaključke.

2 Telesna senzorska omrežja

Telesna senzorska omrežja so v osnovi omrežje nevsiljivih naprav, ki se nahajajo v neposredni bližini telesa, na telesu ali so vgrajene v samo telo, zbirajo fiziološke signale, ki jih proizvaja telo ali druge signale o stanju telesa, ter te podatke posredujejo drugim napravam, ki zatem upravljajo z njimi.

Kar smo v tej dispoziciji združili v poenoteno poimenovanje "telesna senzorska omrežja" – TSO, se v svetovni znanstveni literaturi označuje s številnimi imeni. Najpogostejši obliki imenovanja sta Body Area Network (BAN) in Body Sensor Network (BSN). Obe poimenovanji se pogosto pojavita tudi z besedo Wireless (slo. brezžično), tako da nastaneta oznaki WBAN in WBSN. Ta beseda je sicer pogosto izvzeta in je implicirana že v osnovnem poimenovanju, ker so oblike komunikacije v takšnih okoljih praktično vedno brezžične. Alternativne oblike imenovanja, ki pa niso tako pogoste, zajemajo še Body Area Sensor Network (BASN) [15], Wireless Body Area Sensor Network (WBASN) [16], Body Area Network for Telemedicine (BANT) [17] in Wearable Health-Monitoring Systems (WHMS) [18]. Telesna senzorska omrežja so podskupina brezžičnih senzorskih omrežij (angl. wireless sensor network), zato se zelo pogosto uporabi tudi to poimenovanje. Katero poimenovanje uporabimo, je odvisno predvsem od dela omrežja, ki ga želimo poudariti. Tako obstajajo tudi druga poimenovanja, vendar se ta praviloma uporabljajo, ko govorimo o komunikaciji med akterji (npr. zdravstvenim delavcem in strežnikom), ki zbira in obdeluje podatke – Wireless Medical Sensor Network (WMSN) [19, 20] in Telecare Medicine Information System (TMIS) [21, 22]. V tej nalogi smo se odločili za prevod poimenovanja Body Sensor Network – Telesno Senzorsko Omrežje, ker po našem mnenju najbolje opiše okolje in naprave, na katere smo v disertaciji omejeni. S tem poimenovanjem poudarimo, da so protokoli, o katerih bo govora v disertaciji, namenjeni varovanju komunikacije s senzorskimi napravami, in ne med drugimi napravami, ki so tudi prisotne v sistemu (celostna struktura komunikacije bo predstavljena v poglavju 2.2.1).

Naslednja podpoglavja so namenjena predstavitvi interneta stvari in brezžičnih senzorskih omrežjih, ki so del interneta stvari, ter TSO, ki so nadaljnja podskupina brezžičnih senzorskih omrežij.

2.1 Internet stvari in brezžična senzorska omrežja

Internet stvari je ogromen nabor naprav, ki so povezane v omrežje in komunicirajo z drugimi napravami (angl. machine to machine – M2M). Omrežje takšnih naprav, ki je primarno namenjeno spremljanju oziroma nadzoru določenega okolja, se imenuje brezžično senzorsko omrežje. S časom se je pojavila ideja, da bi takšna omrežja nadzorovala okolje človeškega telesa. S tem se je pojavil TSO kot nova izvedba brezžičnega senzorskega omrežja. To podpoglavje je namenjeno predstavitvi omenjenih konceptov, iz katerih je nastal TSO.

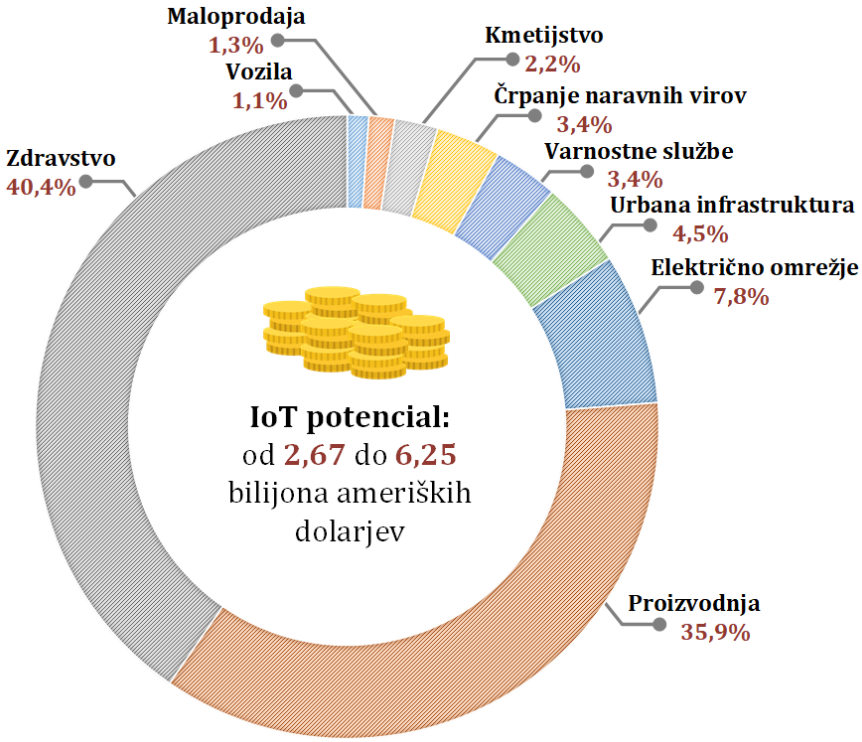
2.1.1 Internet stvari

Internet stvari (angl. Internet of Things – IoT) je omrežje povezanih "stvari" (npr. pametni telefoni, senzorji, pametne hiše, avtomobili, pametne žarnice itd.). Skupna točka vseh teh naprav je njihova sposobnost povezave v internet in izmenjave podatkov z drugimi napravami. To omogoča oddaljeno sledenje, nadzor in upravljanje z napravami preko obstoječe infrastrukture, kar približa digitalni in stvarni svet ter zmanjša človeško posredovanje. Internet stvari je tretja revolucija na področju informacijskih tehnologij, za izumom računalnika in interneta [23]. Začetki poimenovanja interneta stvari segajo v leto 1999, medtem ko Cisco Internet Business Solutions Group ocenjuje začetek interneta stvari med letoma 2008 in 2009, ko je število naprav, povezanih v internet, preseglo svetovno populacijo [24]. Leta 2018 je bilo število naprav, povezanih v internet, ocenjeno na 17,8 milijarde, od tega je 7 milijard IoT-naprav [25]. Rast takšnih naprav naj bi strmo naraščala in podjetje Cisco ocenjuje, da bo do leta 2030 v internet povezanih že 500 milijard naprav [26].

Internet stvari bo oziroma je že spremenil veliko stvari v našem vsakdanjem življenju – kako vozimo, kako sprejemamo odločitve, kako pridobivamo in izrabljamo energijo itd. Vseprisotnost naprav, ki so del interneta stvari, izboljša in poenostavi opravila njegovih uporabnikov. Vendar na drugi strani ta ista lastnost povzroči problematiko zasebnosti in posledično varovanja takšnih omrežij. Ena največjih ovir splošne masovne uporabe interneta stvari je prav varnost in zasebnost podatkov, ki jih te naprave zbirajo in pošiljajo preko omrežja [27]. Ti podatki so lahko občutljive narave, ker so tipično močno vezani na uporabnika oz. njegovo življenje in je posledično mogoče iz njih pridobiti veliko zasebnih informacij. Obstoječe rešitve za varovanje komunikacije so večinoma namenjene uporabi v centraliziranih arhitekturah in so posledično težko prilagodljive za internet stvari. Izziv varovanja je še toliko večji, ker so IoT-naprave tipično omejene z računskimi, pomnilniškimi in energetskimi viri, so heterogene ter so lahko mobilne. IoT-omrežja morajo biti zaradi števila naprav in frekvence dodajanja in odvzemanja naprav tudi bolj razširljiva kot tradicionalna omrežja.

Internet stvari že danes igra pomembno vlogo v našem vsakdanjem življenju na najrazličnejših področjih: zdravstvo, industrija, prevoz, razvedrilo, dom itd. Kljub temu so pričakovanja za rast in izrabo interneta stvari v prihodnosti zelo velika. Internet stvari lahko ustvari novo dodano vrednost za njegove uporabnike na različne načine. Najpogostejši so z izboljšavo produktivnosti v že obstoječih procesih, z omogočanjem novih izdelkov in storitev ter z omogočanjem novih poslovnih strategij. McKinsey Global Institute je izdal poročilo [28], v katerem napoveduje ekonomski potencial, za katerega ocenjujejo, da ga bo tehnologija dosegla do leta 2025. Takšen potencial so izračunali tudi za IoT. Največji doprinos tehnologije se pričakuje na naslednjih področjih: zdravstvo, proizvodnja, pametna električna omrežja, urbana infrastruktura (promet, vodni sistemi, pobiranje smeti itd.), varnostne službe (policija), črpanje naravnih virov (nafta, kovine in minerali), kmetijstvo, maloprodaja in vozila (izboljšanje varnosti in posledična preprečitev škode). Ekonomski potencial vseh panog je bil ocenjen na vrednost od 2,67 do 6,25 bilijona ameriških dolarjev. Največji potencial in zelo velik delež celotnega predvidenega dobička predstavlja prav zdravstvo, del katerega so tudi TSO. Na

spodnji sliki (Slika 2.1) je predstavljeno povprečno razmerje (vzeta je povprečna vrednost med konservativnim in največjim predvidenim potencialom posameznega področja) med ekonomskimi potenciali posameznih panog. V zdravstvu se do leta 2025 pričakuje, da bo uporaba IoT-tehnologij doprinesla vrednost med 1,1 in 2,5 bilijona ameriških dolarjev.



Slika 2.1: Povprečen potencial vpeljave IoT v posamezne panoge [28].

2.1.2 Brezžično senzorsko omrežje

Brezžično senzorsko omrežje (angl. wireless sensor network – WSN) je sestavljeno iz velikega števila prostorsko razpršenih majhnih avtonomnih naprav. Te naprave imenujemo senzorska vozlišča. Sestavljena so iz enega ali več senzorjev, komunikacijskega dela, procesne enote, pomnilnika, vira energije in v nekaterih primerih aktuatorja, preko katerega lahko naprava vpliva na svoje okolje. Zanimanje za brezžična senzorska omrežja se je okrepilo z napredkom v tehnologiji mikro-elektro-mehanskih sistemov (angl. micro-electro-mechanical systems – MEMS), ki omogočajo razvoj pametnih senzorjev [29]. Ti senzorji so majhne naprave z omejenimi procesnimi viri, ki so cenejše od tradicionalnih senzorjev. Omrežje je lahko sestavljeno iz nekaj deset do nekaj tisoč senzorjev, ki so namenjeni pridobivanju podatkov iz okolja. Tako veliko število naprav je potrebno za zagotovitev pokritosti nadzorovanega območja in za zagotovitev zanesljivosti pridobivanja podatkov. Brezžična senzorska omrežja spadajo med tehnologije interneta stvari. Za takšna omrežja so značilni: veliko število naprav (v primerjavi z drugimi oblikami omrežij), mobilnost naprav, možnost okvar, napake v

komunikaciji, dinamično spreminjanje topologije omrežja in omejeni strojni viri. Razlogi za to so velikost senzorskih naprav in stroški proizvodnje tako velikega števila naprav.

Brezžično senzorsko omrežje je namenjeno zaznavanju fizičnih ali okolijskih prametrov, kot so temperatura, vlaga v zraku, zračni pritisk itd., ter omogoča oddaljen nadzor nad območjem. Senzorske naprave zaznavajo spremembe v okolju in te posredujejo med seboj, dokler ti ne pridejo do ponora podatkov (angl. sink) oziroma bazne postaje (angl. base station). Bazne postaje zbirajo podatke več senzorskih naprav, jih združujejo in posredujejo uporabnikom. Brezžična senzorska omrežja tipično nimajo dodatne infrastrukture, ki bi bila potrebna za njihovo delovanje. Omrežja so lahko strukturirana ali nestrukturirana [29]. Nestrukturirana omrežja so sestavljena iz velikega števila gosto in tipično naključno porazdeljenih naprav na nekem območju. Po umestitvi naprav v prostor omrežje ni nadzorovano. Zaradi velikega števila naprav in njihove naključne porazdelitve (ter potencialno tudi geografskih preprek) je upravljanje naprav in povezav ter odkrivanje napak na napravah ali v povezavah praktično nemogoče. Nestrukturirana oblika omrežja je uporabljena predvsem, ko gre za veliko število senzorskih naprav oziroma je potrebno pokriti zelo veliko področje in ko je področje nedostopno ali nevarno za človeka (npr. vulkan). V strukturiranem brezžičnem senzorskem omrežju so naprave nameščene na predvidljiv in predhodno pripravljen način. Prednost takšne namestitve je veliko lažje in posledično cenejše upravljanje in vzdrževanje. Strukturirana porazdelitev senzorskih naprav tudi zagotavlja predvidljivo oziroma celovito pokritost območja z manjšim številom naprav, medtem ko lahko pri naključni porazdelitvi naprav nastanejo območja, kjer ni prisotna nobena naprava.

Brezžična senzorska omrežja lahko razdelimo glede na njihov namen, obliko izmenjave informacij med senzorskimi napravami in čas poročanja [30]. Namen naprav je lahko spremljanje ali spremljanje in reakcija. Pri prvem naprave zgolj zbirajo podatke in te posredujejo naprej, medtem ko pri namenu spremljanja in reakcije naprave preko aktuatorjev glede na podatke, ki jih zbirajo, reagirajo in vplivajo na samo okolje, ki ga opazujejo. Glede na obliko izmenjave informacij v omrežju poznamo komunikacijo "mnogi enemu", ko senzorske naprave pošiljajo podatke eni bazni postaji, oziroma "mnogo mnogim", ko je v omrežju več baznih postaj. Ko pride do obratnega toka podatkov in bazna postaja pošilja navodila senzorskim napravam, gre za komunikacijo "eden mnogim". Poročanje oziroma oddajanje podatkov s strani senzorskih naprav je lahko periodično, ko senzorska naprava posreduje podatke bazni postaji na določeno časovno enoto, ali pa se poročanje sproži ob določenem dogodku, ki ga zazna senzor.

Brezžična senzorska omrežja so se uveljavila kot stroškovno učinkovita in primerna rešitev v številnih rešitvah, namenjenih nadzoru, upravljanju, varovanju in avtomatizaciji. Primarni primeri uporabe takšnih omrežij so: nadzor in opazovanje sprememb v okolju za namene napovedovanja naravnih katastrof (npr. potresov ali požarov), vojaški nadzor in sledenje tarčam, zaznavanje vdora in identifikacije, za nadzor habitatov, za nadzor in upravljanje prometa, za nadzor distribucije in odkrivanje uhajanja vode, električne energije ali zemeljskega plina, za nadzorovanje onesnaženosti voda ali zraka ter za namene spremljanja zdravstvenega stanja ljudi. Zahteve v zdravstvu so nekoliko bolj specifične od preostalih, zato so se oblikovala

telesna senzorska omrežja, ki so podskupina brezžičnih senzorskih omrežij in so specifično namenjena zbiranju in upravljanju s podatki, pridobljenimi iz teles uporabnikov, primarno v zdravstvene namene.

2.2 Pregled področja brezžičnih telesnih senzorskih omrežij

Telesno senzorsko omrežje (TSO) je brezžično omrežje, sestavljeno iz naprav, namenjenih nošenju na telesu, ki se povezujejo z zmogljivejšimi napravami, preko katerih posredujejo podatke v širše omrežje ali internet. Nosljive naprave so biosenzorji (v nadaljevanju samo senzorji), ki so lahko vgrajeni v oblačila, so nameščeni neposredno na telo ali vgrajeni v samo telo [11]. Senzorji zajemajo podatke o stanju telesa in jih posredujejo v omrežje. Te naprave ne obdelujejo podatkov. Senzorji tipično zbirajo fiziološke podatke, kot so srčni utrip, krvni tlak, raven glukoze, elektrokardiogram (EKG), elektromiogram (EMG), elektroencefalogram (EEG) itd., ali druge podatke o stanju telesa, kot je na primer merjenje pospeška, kar je na primer posebej uporabno pri spremljanju športnih aktivnosti ali za ugotavljanje, če je pacient padel. Vsi takšni podatki in še posebej fiziološki podatki so zelo občutljivi oziroma so osebne narave, zato je pomembno, da niso dostopni brez ustreznih razlogov in pooblastil. Te vrste podatkov o uporabniku je tudi mogoče izkoristiti v namene, ki niso v dobrobit uporabnikov. Vsi, ki takšne podatke merijo in hranijo, so zakonsko dolžni upoštevati določena pravila ali minimalne standarde, ki preprečujejo njihovo izkoriščanje. Posledično je potrebno takšne podatke varovati med pošiljanjem in hranjenjem, tako da so zagotovljeni zasebnost (angl. confidentiality), celovitost (angl. integrity) in overjanje pošiljatelja (angl. authenticity).

IEEE 802.15 Task Group 6 [8] definira brezžična TSO kot skupino nizkozmogljivih naprav, ki delujejo v telesu, na telesu ali blizu telesa (ne nujno človeškega) in delujejo v korist uporabnika. Vozlišča oziroma senzorji so lahko nosljive naprave (angl. wearables) ali vsadki (naprave, ki se vsadijo v telo). Prve so tipično večje in imajo posledično večjo napajalno enoto (baterija ali akumulator) in večji pomnilnik ter bolj zmogljivo centralno procesno enoto [31]. Tipični primeri nosljivih naprav so [32]: termometer, senzor dihanja, senzor srčnega utripa, pulzni oksimeter, senzor krvnega tlaka, senzor pH, senzor glukoze itd. Vgrajene naprave, ki so manjše in manj zmogljive, pa se nahajajo v samem telesu in so tipično uporabljene kot [32]: senzor srčne aritmije, senzor intrakranialnega tlaka in endoskopska kapsula. Preko teh naprav lahko avtomatizirano in oddaljeno nadzorujemo zdravstveno stanje uporabnika. Takšen sistem razbremeni zdravstvene delavce nalog opazovanja in nadzora bolnikov, vendar ohranja kakovost zdravstvenih storitev. TSO omogoča neprekinjen nadzor in beleženje uporabnikovega fizičnega stanja brez omejevanja njegove mobilnosti ali udobja. TSO se lahko uporabi za nadzor v domačem okolju ali v bolnišnici, za nadzor vitalnih znakov, za beleženje zdravstvenih podatkov športnikov ali kot del okoliškega sistema (angl. ambient system) [33].

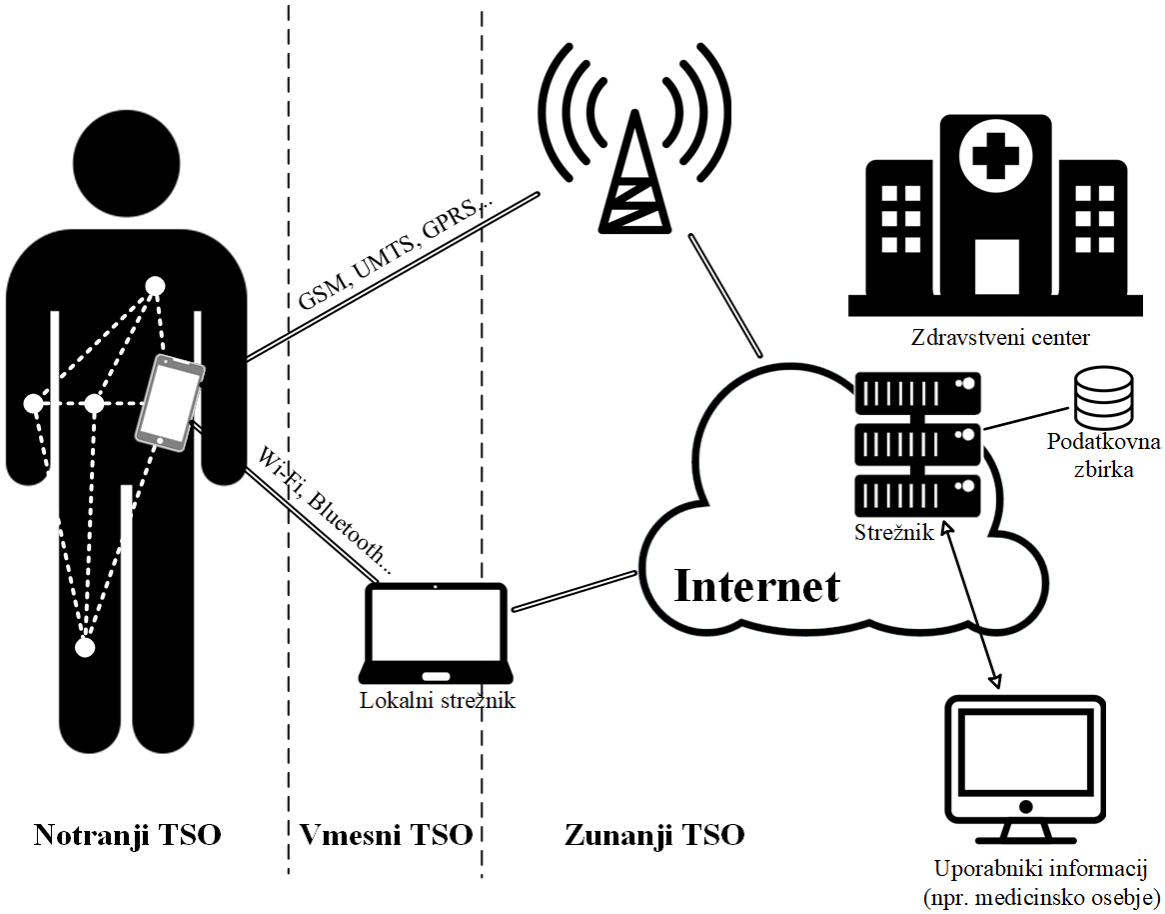
TSO so tipično brezžična omrežja, vendar obstajajo tudi alternativni mediji prenosa. Predlagane so bile rešitve za komunikacijo preko samega telesa uporabnika (angl. intrabody

communication) z uporabo električnih signalov [34] ali preko vibracij, ki se širijo po telesu in tako prenašajo podatke med dvema napravama [35].

Pokazatelj, da so TSO postala pomembna razlikovalna domena, je število preglednih člankov, ki obravnavajo različne dele domene in so bili objavljeni v znanstvenih revijah. Tukaj so našteti nekateri bolj pomembni pregledni članki [6, 11, 16, 18, 31, 36–55]. Naslavljajo različna področja TSO, kot so strojna oprema, problemi in izzivi, ki jih je potrebno nasloviti, preden lahko postane tehnologija splošno uporabna, motnje v komunikaciji, kvaliteta storitev itd.

2.2.1 Struktura komunikacije

Struktura komunikacije v tipičnem TSO, ki je namenjeno uporabi v zdravstvene namene, je razdeljena na tri dele [16]. Prvi del se imenuje notranji TSO (angl. intra-BAN) in predstavlja dejansko TSO. Sestavljajo ga senzorske naprave, ki so nameščene v telo, na telo in okrog telesa, ter osebni strežnik (angl. personal server). Kot je že bilo omenjeno, so senzorske naprave zelo omejene v svoji velikosti in so zato tudi manj zmogljive. Lahko so posredniki za druge senzorske naprave, ki jim je osebni strežnik zunaj dosega. Osebni strežnik je tipično pametni telefon ali pametna ura, ki zbira podatke iz senzorjev in jih posreduje naprej. Osebni strežnik je zmogljivejša naprava od senzorjev, zato je tudi primeren za opravljanje vloge posrednika. Naslednji nivo strukture komunikacije TSO je vmesni TSO (angl. inter-BAN). V tem nivoju se nahaja lokalni strežnik (angl. local server), ki povezuje več notranjih TSO. Ta nivo je namenjen komunikaciji med različnimi TSO. Osebni strežnik lahko preko lokalnega strežnika tudi posreduje podatke zdravstvenim ustanovam. Takšna komunikacija je manj zahtevna kot neposredna komunikacija med osebnim strežnikom in zdravstvenimi ustanovami. Tretji del je zunanji TSO (angl. beyond-BAN), ki združuje brezžična omrežja in mestna omrežja (angl. metropolitan area networks) za posredovanje podatkov do oddaljenih zdravstvenih ustanov, kjer se podatki zbirajo in obdelujejo. Opisana trinivojska struktura je prikazana na naslednji sliki (Slika 2.2). Alternativna struktura TSO razdeli komunikacijo na dva dela [51]. Notranji TSO ostane enak kot v prejšnji razporeditvi, medtem ko se vmesni in zunanji TSO združita v en sam nivo, ravno tako imenovan zunanji TSO.

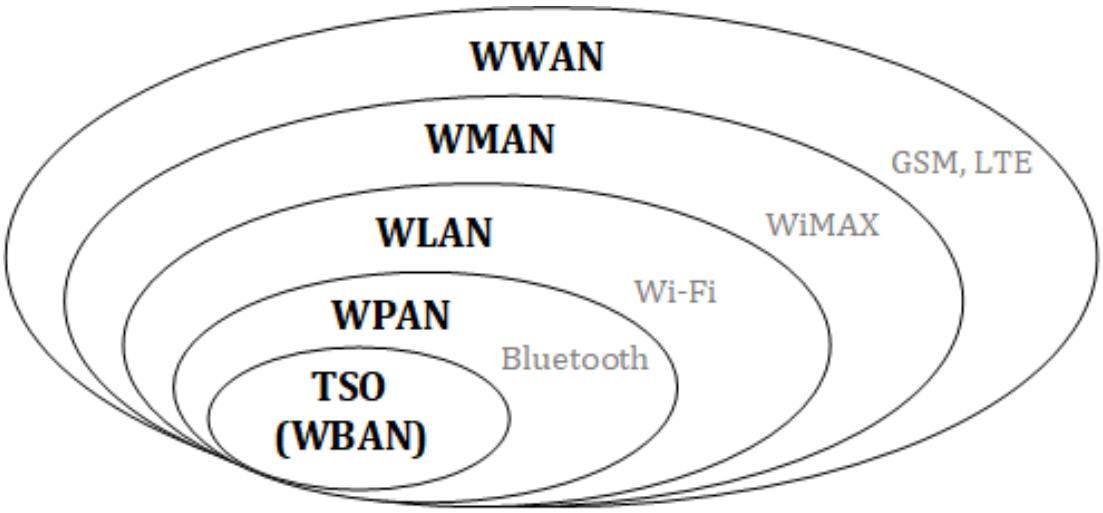


Slika 2.2: Struktura komunikacije [56].

2.2.2 Umestitev TSO med druge vrste omrežij

Poznamo veliko različnih oblik omrežij. Brezžična omrežja so najpogosteje razdeljena v štiri skupine, kjer sta domet signala in namen uporabe glavni merili razlikovanja med njimi. TSO je omrežje kratkega dometa. TSO imajo domet 1-2 m oziroma področje telesa [57]. Brezžično osebno omrežje (angl. Wireless Personal Area Network – WPAN) ima okrog 10 m dosega in tipično ni namenjeno za uporabo v zdravstvene namene. Tipična predstavnika tehnologij v takšnih omrežjih sta Bluetooth in Zigbeee. Naslednje omrežje je brezžično lokalno omrežje (angl. Wireless Local Area Network – WLAN), ki je namenjeno pokrivanju enega prostora oz. ene zgradbe. Doseg je do 30 m v prostorih in 100 m na prostem. Tehnologija, ki se uporablja v brezžičnih lokalnih omrežjih, je osnovana na podlagi družine standardov IEEE 802.11 in se imenuje Wi-Fi. Naslednji tip brezžičnega omrežja so brezžična mestna omrežja (angl. Wireless Metropolitan Area Network – WMAN). Njihov doseg je približno 5 km. Tehnologija, ki se tu uporablja, je WiMAX (angl. Worldwide Interoperability for Microwave Access) in izhaja iz standardov 802.16. Omrežje, ki ima najdaljši doseg (nekaj 10 km), je brezžično prostrano omrežje (angl. Wireless Wide Area Network – WWAN). Takšna omrežja tipično uporabljajo tehnologije mobilnih omrežij, kot so GSM (Global System for Mobile communications), GPRS (General Packet Radio Service), UMTS (Universal Mobile Telecommunications System), LTE

(Long-Term Evolution) itd. Spodnja slika (Slika 2.3) kaže umestitev TSO med preostale tipe brezžičnih omrežij.



Slika 2.3: Umestitev TSO v brezžična omrežja [57, 58].

2.2.3 Primerjava telesnih senzorskih omrežij in brezžičnih senzorskih omrežij

Primarna razlika med TSO in brezžičnim senzorskim omrežjem (predstavljeno v poglavju 2.1.2) je entiteta, o kateri senzorske naprave zbirajo podatke. Brezžična senzorska omrežja zbirajo podatke o okolju (npr. temperatura, vlaga v zraku ipd.), medtem ko je TSO namenjen zbiranju podatkov o stanju telesa. TSO so specifična oblika brezžičnega senzorskega omrežja, ki je tipično asociirano s človeškim telesom, čeprav ni omejeno za uporabo samo na ljudeh. TSO pokriva veliko manjše fizično področje in posledično vsebuje manjše število naprav. Redundantne naprave so v TSO nezaželene. To in dejstvo, da se v TSO lahko pošiljajo kritični podatki za preživetje posameznika, zahteva veliko večjo odpornost omrežja na izgube med prenosom ter natančnost meritev. Nobena od teh lastnosti ni tako strogo zahtevana v brezžičnih senzorskih omrežjih. Ker v TSO ni redundantnih naprav, to pomeni, da so si naprave v istem omrežju med seboj lahko zelo različne, medtem ko so v brezžičnem senzorskem omrežju naprave pogosto enake (merijo isti pojav na različnih lokacijah). Ne glede na to sta obe vrsti omrežij omejeni v virih, s katerimi naprave razpolagajo. To je primarno posledica velikosti senzorskih naprav. Naprave v brezžičnih senzorskih omrežjih so praviloma nekoliko manj omejene glede velikosti, kot so naprave v TSO, kar pomeni, da so te naprave praviloma tudi nekoliko bolj zmogljive in imajo večjo napajalno enoto, medtem ko so naprave v TSO najpreprostejše glede zmogljivosti, čeprav to ne pomeni, da so preproste za proizvodnjo (npr. zaradi kompaktnosti komponent in zahtev po uporabi telesu prijaznih materialov). Topologija omrežja se v brezžičnih senzorskih omrežjih tipično ne spreminja, medtem ko so TSO-naprave nameščene na telo in posledično pogosto v gibanju, kar lahko glede na vidljivost med napravami spreminja tudi topologijo. Iz tega razloga je za TSO potrebno razviti tudi

specializirane komunikacijske protokole, ki podpirajo takšne spremembe v topologiji [57]. Premikanje TSO tudi pomeni, da ta pogosto pridejo v stik z drugimi TSO, kar je dodaten razlog za zagotavljanje robustnosti komunikacije kljub motnjam, ki nastanejo zaradi prekrivanja dveh ali več omrežij. Razlika med obema vrstama omrežij je tudi v razširljivosti oziroma nadomeščanju naprav. Brezžična senzorska omrežja so lažje razširljiva in ob prenehanju delovanja naprav se lahko dodajo nove naprave, brez odstranitve starih (zaradi zahtevne dostopnosti do naprav), medtem ko je dodajanje naprav v TSO bolj redko in je v primeru zamenjave senzorske naprave, starejšo napravo potrebno odstranit. Čeprav so brezžična senzorska omrežja in TSO sorodna omrežja, so razlike med obojimi dovolj velike, da protokoli, ustvarjeni za uporabo v enem od tipov omrežja, niso primerni za uporabo v drugem. Na naslednji tabeli (Tabela 2.1) je prikazan pregled pomembnih razlik med brezžičnimi senzorskimi omrežji in TSO.

Tabela 2.1: Razlike med TSO in brezžičnimi senzorskimi omrežji [51, 53].

Lastnost	**Brezžično senzorsko omrežje**	**Telesno senzorsko omrežje**
Obsežnost	Nadzorovano okolje (od nekaj metrov do nekaj kilometrov).	(Človeško) telo (od nekaj centimetrov do nekaj metrov).
Število vozlišč	Veliko število (redundantnih) vozlišč za pokritje velikega področja.	Majhna količina, omejen prostor, brez redundance.
Natančnost meritev	Posamezne meritve niso natančne. Natančnost se doseže s povprečjem meritev redundantnih naprav.	Potrebna so natančna in robustna vozlišča.
Posledice izgube podatkov	Tipično ni posledic, izgubljeno se nadomesti s podatki drugih vozlišč.	Posledice so lahko pomembne, lahko se zahtevajo ponovne meritve za zagotavljanje kakovosti prenosa.
Naloge vozlišč	Vozlišča imajo tipično specifično nalogo.	Vozlišča najpogosteje opravljajo več nalog.
Mobilnost	Naprave v brezžičnih senzorskih omrežjih so tipično stacionarne, topologija se ne spreminja.	Naprave v TSO se premikajo skupaj s telesom. Naprave, nameščene na okončinah, se premikajo drugače kot naprave, nameščene na trupu. To lahko povzroči tudi dinamične spremembe v topologiji omrežja. Premikanje posameznikov pomeni, da se omrežja različnih uporabnikov pogosto prekrivajo.
Zamenjava vozlišča	Sama zamenjava je preprosta, dostop do vozlišč je lahko težaven, vozlišča so namenjena enkratni uporabi brez potrebe zbiranja	V primeru vsadkov zahtevna in draga zamenjava.

	naprav potem, ko niso več v uporabi.	
Podatkovni prenos	Tipično enakomeren – ni obdobij velikega prenosa podatkov in obdobij majhnega prenosa podatkov.	Tipično neenakomeren – podatki se pošiljajo glede na uporabnikovo stanje oziroma aktivnost. Posledično je podatkovni prenos nepredvidljiv in lahko vključuje obdobja visokega prenosa.
Napajanje	Omejeno, vendar v manjši meri. Lažja in bolj pogosta možnost menjave baterije, če okolje to dopušča.	Omejeno. Zelo zahtevna in draga zamenjava v vsadkih.
Biokompati-bilnost	Praktično nikoli potrebna.	Zahtevana za vsadke in naprave v neposrednem stiku s telesom.
Pomembnost varovanja komunikacije	Nižja.	Višja (varovanje osebnih podatkov).

3 Protokoli za overjanje in dogovor o ključu

Poglavje je namenjeno predstavitvi konceptov, povezanih z overjanjem in dogovorom o ključu. To vključuje predstavitev različnih oblik overjanja in vzpostavitve. Poglavje vključuje tudi predstavitev osnovnih kriptografskih gradnikov, ki bodo omenjeni v disertaciji in poznavanje katerih je pomembno za razumevanje delovanja protokolov overjanja in vzpostavitve ključa, razvitih v tej doktorski disertaciji.

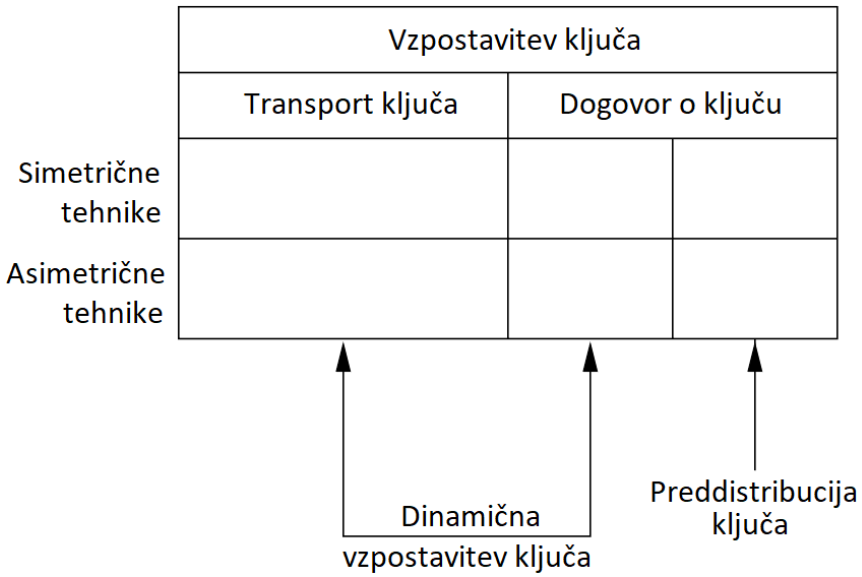
3.1 Vzpostavitev ključa

Vzpostavitev ključa ali izmenjava ključa (angl. key establishment ali key exchange) je proces, v katerem se skrivnost oziroma ključ, namenjen kriptografski uporabi, deli med dve ali več entitet [59]. Vzpostavitev ključa je prvi in najpomembnejši element zagotavljanja zaupnosti podatkov, istovetnosti deležnikov in celovitosti sporočil v varni komunikaciji. Namen je vzpostaviti varno povezavo med entitetami, ki sodelujejo v komunikaciji, in preprečevanje drugim, da bi tej komunikaciji prisluškovali ali vanjo posegali. Dogovor o ključu (angl. key agreement) je protokol oziroma mehanizem, ki omogoča vzpostavitev deljene skrivnosti med dvema ali več entitetami na način, da vse vključene entitete na nepredvidljiv način prispevajo k izgradnji te skrivnosti. Dogovor o ključu je oblika vzpostavitve ključa. Druga oblika vzpostavitve ključa je transport oziroma prenos ključa (angl. key transport), kjer skrivnost ustvari ena od entitet, vključenih v vzpostavitev. Ta entiteta nato posreduje ustvarjeno skrivnost preostalim deležnikom. Razlika med obema oblikama vzpostavitve ključa je torej v sodelovanju deležnikov pri izgradnji skrivnosti. Pri dogovoru o ključu sodelujejo vse entitete (na nepredvidljiv način), medtem ko pri transportu ključa skrivnost ustvari ena sama entiteta, ki zatem ustvarjen ključ posreduje preostalim deležnikom. Upravljanje s ključi je tretja oblika (angl. key mamagement), ki poleg ustvarjanja in izmenjave ključa vključuje še hranjenje in zamenjavo ključa.

Pri vzpostavitvi ključa ločimo med protokoli s predporazdeljenimi ključi (angl. pre-distributed key) in dinamično vzpostavljenimi ključi (angl. dynamic key establishment) [59]. Pri uporabi predporazdeljenih ključev se ključi (oz. material, namenjen za izdelavo ključev) namestijo na naprave, preden se te predajo v uporabo. V takšnih primerih je vzpostavljen ključ odvisen od predporazdeljenih podatkov. Rezultat protokola s predporazdeljenimi ključi je tipično trajni ključ. Kot že ime nakazuje, se trajni ključ ne spreminja, čeprav se lahko uporabi tudi za vzpostavitev sejnega ključa. Dinamično vzpostavljen ključ se razlikuje oziroma je unikaten ob vsaki vzpostavitvi ključa. Dinamična vzpostavitev ključa ustvari deljeno skrivnost med deležniki, ki jo imenujemo sejni ključ (angl. session key). Sejni ključ se dejansko uporabi za šifriranje komunikacije in je praviloma namenjen kratkotrajni uporabi (npr. eni sami povezavi med napravami ali eni seji). Po izteku namena sejnega ključa se ta ne uporablja več in se ne

hrani na napravah. Kratkotrajna uporaba sejnih ključev ima kot posledico veliko pozitivnih učinkov. Z večanjem količine podatkov, ki so šifrirani z istim ključem, se povečuje referenčni material, na podlagi katerega lahko napadalec izvede kriptoanalizo. Redno spreminjanje sejnega ključa omeji količino podatkov, šifriranih z istim ključem. Manjša količina podatkov, šifriranih z istim ključem, pomeni tudi, da se v primeru razkritja sejnega ključa razkrije manjši del komunikacije. Uporaba sejnih ključev zagotavlja tudi neodvisnost med sejami. Razkritje sejnega ključa ne vpliva na varnost podatkov, ki so bili zavarovani z drugimi sejnimi ključi. Dodatno kratkotrajni ključi tudi zmanjšajo zahteve po dolgotrajnem hranjenju ključev, saj je potrebno hraniti samo ključe, ki so dejansko v uporabi.

Za vzpostavitev ključa preko javnega kanala je treba zagotoviti zaupnost, ki se doseže z uporabo šifre. Ko govorimo o varovanju zaupnosti, je prva rešitev vedno simetrično šifriranje (angl. symmetric encryption). Simetrično šifriranje je relativno hitro, potrebuje majhne količine pomnilnika in ni računsko zahtevno [60]. Kot takšno je primerno tudi za uporabo v TSO. Pomanjkljivost simetričnih šifrirnih protokolov je uporaba enakega ključa za šifriranje in dešifriranje, kar pomeni, da morata napravi v komunikaciji posedovati ta ključ, preden lahko varno izmenjujeta sporočila. To je težava v brezžičnih omrežjih, kot je TSO, ki so še posebej dovzetna na napad vrinjenega napadalca (angl. Man in The Middle Attack – MiTM). Za preprečevanje vrinjenega napadalca v proces izmenjave ključa se tipično uporabi asimetrično šifriranje z notranjim ali zunanjim certifikacijskim organom. V tradicionalnih sistemih se zato asimetrične tehnike tipično uporabljajo za namene vzpostavitve ključa, medtem ko se simetrične šifre primarno uporabljajo za šifriranje dejanskega prenosa podatkov. Vendar omejitve, ki so prisotne v TSO, preprečujejo uporabnost asimetrične kriptografije, ki je računsko in energetsko zelo zahteven način izmenjave ključa. Dinamično vzpostavitev ključa in preddistribucijo ključa lahko dosežemo z uporabo različnih kombinacij oblik vzpostavitve ključa (dogovor ali transport ključa) in vrste uporabljenega šifriranja (simetrično ali asimetrično). Posamezno tehniko vzpostavitve ključa lahko na takšen način klasificiramo. Klasifikacija je prikazana na naslednji sliki (Slika 3.1).



Slika 3.1: Preprosta klasifikacija tehnik vzpostavitve ključa [59].

Tipičen primer uporabe asimetričnega algoritma za namen transporta dinamičnega ključa je infrastruktura javnega ključa (angl. public key infrastructure – PKI), kjer se javni ključ pridobi s spleta in se zato lahko prosto spreminja, medtem ko je vzpostavljen ključ poljubna naključna vrednost. Primer dogovora o ključu z uporabo asimetrične tehnike za izgradnjo dinamičnega ključa je Diffie-Hellmanov protokol. Tu gre za dogovor o ključu, ker že sam Diffie-Hellmanov protokol zahteva uporabo vrednosti, ki jih ločeno ustvari vsaka entiteta v komunikaciji. Uporaba asimetrične tehnike s preddistribucijo za namene dogovora o ključu je dosežena s predčasno nameščenim javnim ključem asimetričnega šifrirnega algoritma (npr. RSA), ki pa ga ni mogoče dinamično spremeniti, tako kot je to bilo možno ob uporabi infrastrukture javnega ključa. V nasprotju z uporabo asimetrične kriptografije je simetrična kriptografija veliko bolj učinkovita, predvsem ko gre za računsko kompleksnost, in posledično bolj zaželena v sistemih z omejeno računsko močjo, kot je tudi TSO. Dobro poznan primer uporabe simetričnih tehnik za namen transporta ključa je protokol Kerberos. Protokol, ki tudi spada v to skupino, bo predstavljen v poglavju 6.2. Primer protokola za dogovor o dinamičnem ključu na osnovi simetričnih tehnik je Blomova shema. Drugi primer protokola iz te skupine bo predstavljen v poglavju 7.1 (zgoščevalne funkcije se uvrščajo med simetrične algoritme). Oba protokola, ki bosta predstavljana v nadaljevanju (poglavji 6.2 in 7.1), sta rezultat lastnih raziskav in znanstveni doprinos te disertacije. Kot dogovor o ključu s predporazdeljenim ključem in ob uporabi simetričnih tehnik lahko štejemo simetričen ključ, ki je predčasno nameščen na naprave. To je zelo primitiven način vzpostavitve ključa, ki ni primeren za uporabo v omrežjih z večjo količino komunikacije. Modernejše oblike takšnega delovanja so bazeni ključev (angl. key pool) in verige ključev (angl. key chain), ki omogočajo predporazdelitev več različnih ključev.

3.2 Overjanje

Overjanje ali preverjanje pristnosti (angl. authentication) je funkcionalnost, ločena od dogovora o ključu, vendar je redno uporabljena pri vzpostavitvi ključa. Overjanje je proces preverjanja istovetnosti. Ločimo med overjanjem entitet oziroma vozlišč, overjanjem ključev in potrjevanjem ključev [59]. Overjanje entitet oziroma overjanje vozlišč (angl. entity authentication ali node authentication) je proces, v katerem entiteta preko pridobljenega dokaza preveri pristnost in aktivnost druge entitete, vključene v komunikacijo. Medsebojna overitev (angl. mutual authentication) je razširitev tega procesa, tako da vse entitete, vključene v protokol, preverijo pristnost vseh ostalih entitet. Podobno overjanju entitet je tudi overjanje izvora sporočila (angl. message authentication ali data origin authentication). To je oblika overjanja, pri kateri se preveri pristnost izvora oz. pošiljatelja sporočila. Overjanje izvora sporočila se od overjanja entitete razlikuje v času preverjanja. Overjanje entitete se izvaja v realnem času, medtem ko se overjanje izvora poročila lahko izvaja tudi za sporočila, poslana v preteklosti. Druga razlika je, da overjanje sporočila preveri samo posamezno sporočilo,

medtem ko se entiteta overi za trajanje celotne seje. Overjanje izvora sporočila samodejno vključuje preverjanje celovitosti (angl. integrity), ki zagotavlja, da se podatki od njihovega nastanka niso na nedovoljen način spremenili. Overjanje ključa (angl. key authentication) je lastnost ključa, s katero se entiteta v komunikaciji zadovolji, da je ključ lahko znan samo drugim entitetam v komunikaciji (in zaupanja vrednim tretjim entitetam, v sistemih, kjer so takšne entitete prisotne). Potrjevanje ključa (angl. key confirmation) je proces, v katerem se entiteta prepriča, da ima druga entiteta v komunikaciji dostop do določenega skrivnega ključa. Ko sta izpolnjeni lastnosti overjanja ključa in potrjevanja ključa, govorimo o eksplicitnem overjanju ključa (angl. explicit key authentication). V nadaljevanju disertacije se bomo z izrazom overjanje sklicevali na overjanje entitete, ostale oblike overjanja pa bodo specifično naslovljene.

3.3 Kriptografski gradniki protokolov overjanja in vzpostavitve ključa

V tem poglavju bodo predstavljene različne kriptografske operacije, ki so pogosto omenjene v disertaciji in so pomembni gradniki različnih protokolov za overjanje in vzpostavitev ključa, tudi tistih, predstavljenih v tej disertaciji.

3.3.1 Osnovni gradniki in operacije

Spajanje

Spajanje oz. konkatenacija (angl. concatenation) je operacija združevanja nizov enega za drugim, na primer spajanje nizov "primer" in "1234" ustvari nov niz "primer1234". V tej nalogi se spajanje pogosto uporabi za združevanje več vrednosti v eno samo vrednost, ki je zatem uporabljena kot vhodna vrednost v operacijo, ki sprejme samo en vhodni parameter (npr. zgoščevalna funkcija). Spajanje je tako preprosta operacija, da se praviloma v analizah učinkovitosti sploh ne omenja.

Enkratna vrednost

Enkratna vrednost (angl. nonce) je vrednost, namenjena enkratni uporabi za dani namen [59]. Enkratne vrednosti se primarno uporabljajo za zagotavljanje svežine sporočil (opisano v poglavju 4.1). V varnostnih protokolih je vedno potrebno zagotavljati celovitost enkratnih vrednosti. Zagotavljanje celovitosti je potrebno, sicer lahko napadalec uporabi stara sporočila, v katerih nadomesti zastarele enkratne vednosti z novimi. Enkratne vrednosti so lahko naključne vrednosti, zaporedna števila ali časovni žigi (angl. timestamp). Naključna vrednost se pošlje v sporočilu in pričakuje v povratnem sporočilu. Naključna vrednost deluje kot povezava med sporočili. Odgovor na prvotno sporočilo je posledično svež, saj je moral biti ustvarjen potem, ko je prejemnik prvega sporočila prejel naključno vrednost. Uporaba naključne vrednosti zagotavlja edinstvenost in nepredvidljivost sporočil ter posredno tudi

pravočasnost. Pri uporabi naključne vrednosti je potrebno hranjenje te vrednosti, dokler je v uporabi (dokler naprava ne prejme povratnih sporočil, v katerih pričakuje to vrednost, ali dokler ne pride do prekinitve povezave). Enkratna vrednost je tipično naključna ali psevdonaključna vrednost. Zahtevana naključnost enkratne vrednosti je odvisna od njenega namena. Uporaba naključnih vrednosti v varnostne namene pogosto zahteva generiranje kriptografsko varnih naključnih vrednosti (dovolj visoka entropija). Zaporedna števila so oblika enkratne vrednosti, v kateri deležniki sledijo predčasno določeni obliki številčenja. Vsako sporočilo je sprejeto le, če je uporabljeno zaporedno število večje od predhodnega in je bila uporabljena dogovorjena oblika številčenja. Najpreprostejša oblika tega je števec, ki ima osnovno vrednost nič in se iterativno povečuje za ena ob vsakem nadaljnjem sporočilu. Zaporedno število mora biti specifično za vsak par naprav v komunikaciji. Naprave morajo hraniti informacije, na podlagi katerih lahko določijo veljavna zaporedna števila. Uporaba zaporednih števil v osnovi ne omogoča zaznavanja zakasnitev. Časovni žig zagotavlja edinstvenost in pravočasnost sporočil. Pošiljatelj pripne časovni žig sporočilu in ga pošlje. Prejemnik na podlagi prejetega časovnega žiga in trenutnega časa izračuna razliko med obema. Če je ta vrednost znotraj sprejemljivega razpona (glede na potreben čas prenosa, čas obdelave podatkov in odstopanja med meritvami časa na obeh napravah), naslovnik sprejme sporočilo, sicer se to zavrne kot staro sporočilo. Ker je časovno okno veljavnosti sporočila majhno, napadalci ne morejo takšnih sporočil ponavljati. Uporaba časovnih značk zahteva, da sta uri na napravah v komunikaciji usklajeni. Alternativno lahko prejemnik sporočil sprejme tudi vsako sporočilo, ki ima edinstven časovni žig (sporočilo s takšnim časovnim žigom ni bilo prejeto nikoli pred tem), vendar mora pri takšnem načinu delovanja prejemnik dodatno hraniti tudi seznam vseh prejetih časovnih žigov.

Bitni operator XOR

Bitni operator XOR (⊕), ki je poznan tudi pod imenoma ekskluzivni ali in izključujoči ali (angl. exclusive or ali exclusive disjunction), sprejme dva bitna vhodna podatka enake dolžine in združi istoležeče bite v izhodne bite [59]. Rezultat vsake od teh operacij XOR je 1, če sta vrednosti istoležečih bitov različni, in 0, če sta vrednosti enaki. Primer: 1010 ⊕ 1100 = 0110. Operacija XOR ima naslednje lastnosti, ki veljajo za vse bitne vrednosti (ali nize bitov) a, b in c:

- $a \oplus a = 0$ (inverz); $a \oplus a \oplus a = a$; $a \oplus 0 = a$ (nevtralni element); $a \oplus 1 = \sim a$, kjer je ~ eniški komplement (angl. bitwise complement); $a \oplus b = b \oplus a$ (komutativnost); $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ (asociativnost); in če je $a \oplus b = c$, potem je $c \oplus b = a$ in $c \oplus a = b$.
- Kot posledica lastnosti iz prve točke izhaja, da ko poznamo $(a \oplus b)$ in a, potem lahko pridobimo vrednost b kot $(a \oplus b) \oplus a = b$. Enako velja za primer, kjer poznamo $(a \oplus b)$ in b in lahko določimo vrednost a kot $(a \oplus b) \oplus b = a$. Ta lastnost se posploši na poljubno število vrednosti, npr. za primer vrednosti a, b, c in d, kjer poznamo $(a \oplus b \oplus c \oplus d)$ in katerekoli tri vrednosti, lahko četrto in nepoznano vrednost pridobimo iz poznanih vrednosti.

Operacija XOR je pogosto uporabljena v kriptografiji, ker je preprosta za razumevanje in analizo ter zelo hitra za izvajanje (še posebej v strojni implementaciji). Ob poznavanju rezultata operacije in delnih vhodnih podatkov (kot je bilo opredeljeno v drugi točki) je izračun neznane vrednosti hiter in preprost. Hkrati je ob poznavanju samo rezultata operacije računsko nemogoče ugotoviti vhodne podatke, ki so ga tvorili.

3.3.2 Kriptografska zgoščevalna funkcija

Zgoščevalna funkcija (angl. hash function) sprejme kot vhod niz bitov poljubne dolžine in ustvari rezultat fiksne dolžine (dejanska dolžina je odvisna od algoritma), ki ga imenujemo izvleček, zgoščena vrednost ali zgostitev (angl. hash ali message digest) [59]. Za dane vhodne podatke je zgoščena vrednost vedno enaka. Kriptografska zgoščevalna funkcija (angl. cryptographic hash function) je enosmerna (angl. one-way function), kar pomeni, da ni obrnljiva (angl. invertable) – iz vhoda je relativno preprosto izračunati rezultat funkcije, vendar je iz rezultata računsko nemogoče pridobiti vhodne podatke. Kriptografska zgoščevalna funkcija mora izpolnjevati naslednje tri lastnosti, kjer je zgoščena vrednost $h = H(x)$, H je kriptografska zgoščevalna funkcija in x je predslika od h [59]:

- Odpornost na predsliko (angl. pre-image resistance): za dani h je računsko nemogoče najti takšen x, da bo $H(x) = h$. Ta lastnost predstavlja enosmernost funkcije.
- Odpornost na drugo predsliko (angl. second pre-image resistance ali weak collision resistance): za dani x je računsko nemogoče najti $y \neq x$, da bo $H(y) = H(x)$.
- Odpornost na trke (angl. collision resistance ali strong collision resistance): računsko nemogoče je najti par različnih sporočil x in y, da bo $H(x) = H(y)$. Prejšnja lastnost zagotavlja, da je za specifično sporočilo računsko nemogoče najti takšno drugo sporočilo, da bosta izvlečka obeh enaka. Odpornost na trke razširi ta pogoj na poljuben par sporočil (prvo sporočilo ni podano). Prva zahtevana lastnost (odpornost na predsliko) je tudi omejena na specifičen izvleček, za katerega mora napadalec najti sporočilo, ki se preslika vanj. Zagotavljanje odpornosti na trke je zato med tremi lastnostmi najzahtevnejše.

Tipični primeri uporabe kriptografske zgoščevalne funkcije so v digitalnih podpisih in pri zagotavljanju celovitosti. Bolje poznane zgoščevalne funkcije so MD5, SHA-1, SHA-2, SHA-3, BLAKE2 in KangarooTwelve. V nadaljevanju se bomo s poimenovanjem zgoščevalne funkcije sklicevali izključno na kriptografske zgoščevalne funkcije.

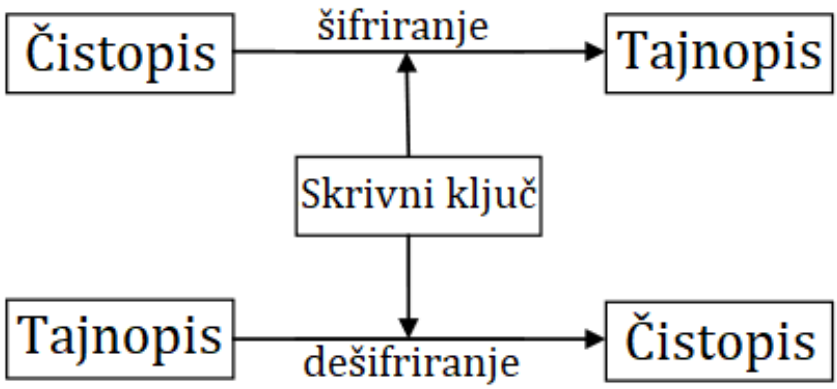
Koda za overitev sporočila (angl. message authentication code – MAC) [59] je funkcija, podobna zgoščevalni funkciji – enosmerna funkcija, ki sprejme podatke poljubne dolžine in proizvede rezultat fiksne dolžine. Vendar funkcija MAC pri vhodu zahteva tudi skrivni ključ, s pomočjo katerega proizvede rezultat, imenovan značka (angl. tag). Kdorkoli želi to značko preveriti, mora tudi poznati ključ, sicer bo rezultat funkcije drugačen. Značka zagotavlja celovitost sporočila (tako kot zgoščena vrednost) in overjanje pošiljatelja, za razliko od digitalnega podpisovanja (angl. digital signature) pa ne zagotavlja nezanikanja (angl. non-repudiation).

Algoritmi MAC so lahko namenski, zgrajeni na osnovi zgoščevalne funkcije (angl. hash-based message authentication code – HMAC) ali na osnovi bločne simetrične šifre (angl. cipher-based message authentication code – CMAC).

3.3.3 Simetrična šifra

Simetrična šifra (angl. symmetric cipher) je algoritem, ki s pomočjo skrivnega ključa šifrira čistopis (angl. plaintext) v tajnopis (angl. ciphertext) [59]. Simetričen ključ je skrivnost, deljena med entitetami v komunikaciji, od katere je odvisna zaupnost podatkov. Isti skrivni ključ se uporabi tudi pri dešifriranju sporočila. Shema delovanja simetričnih šifer je predstavljena spodaj (Slika 3.2).

Uporaba istega ključa za namene šifriranja in dešifriranja je izvor poimenovanja šifre in tudi najpomembnejša pomanjkljivost simetričnih šifer. Ključ mora ostati za vedno skriven, sicer je zaupnost sporočil, ki so bila šifrirana ob njegovi uporabi, izgubljena. Uporaba istega ključa za šifriranje in dešifriranje povzroči tudi težavo njegove distribucije preko javnih kanalov. Rešitev te težave so protokoli za vzpostavitev ključa. Prednost simetričnih ključev pa je predvsem nizka kompleksnost v primerjavi z asimetričnimi šiframi, kar se neposredno pokaže v hitrosti delovanja. Hitrost delovanja pa vpliva tudi na porabo energije pri izvajanju operacij, kar je zelo pomembno na področju protokolov, primernih za uporabo v TSO. Posledično so simetrične šifre edina učinkovita rešitev za zagotavljanje zaupnosti večjih količin podatkov (tudi v sistemih brez strojnih omejitev).



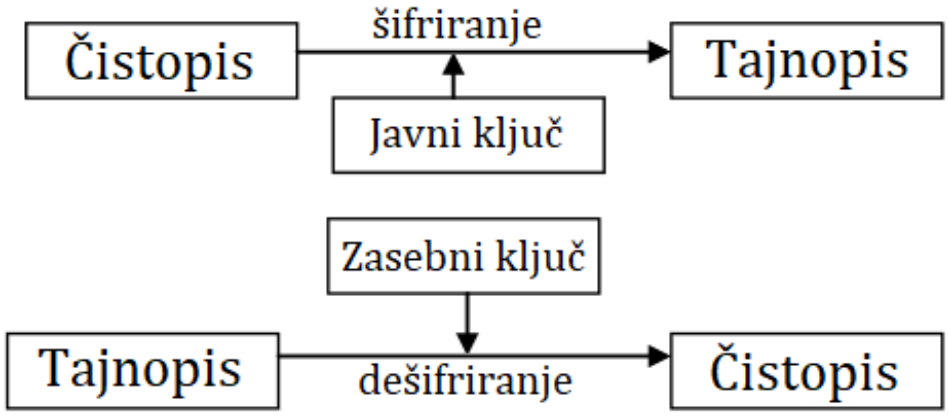
Slika 3.2: Postopek simetričnega šifriranja.

Simetrične šifre se delijo na tokovne (angl. stream cipher) in bločne šifre (angl. block cipher) [59]. Tokovne šifre delujejo tako, da posamezne znake (tipično velikosti bita ali zloga (angl. byte)) čistopisa združijo (tipično z operacijo XOR) z istoležečim znakom toka ključev (angl. keystream), ki je naključen ali psevdonaključen niz znakov, ustvarjen na podlagi skrivnega ključa. Rezultat tega je tajnopis. Bločne šifre šifrirajo določeno količino podatkov naenkrat. To omejeno količino podatkov imenujemo blok. Če količina podatkov presega velikost bloka (ki so praviloma zelo majhni; tipična velikost je 128 bitov), se naslednji blok šifrira z istim ključem in ob enakih pogojih. To prinaša ponovno uporabo ključa, in kot smo že omenjali pri sejnih

ključih, je ponovna uporaba nezaželena. To težavo odpravi način šifriranja (angl. mode of operation), ki omogoča razširitev uporabe enega ključa na praktično poljubno dolžino podatkov. Tudi najboljši simetrični bločni šifrirni algoritmi niso varni za uporabo brez vključitve primernega načina šifriranja. Med nekaj bolje poznanih simetričnih šifer štejemo: AES, Twofish, Serpent, Blowfish, RC4, DES, 3DES in IDEA. Primeri načinov šifriranja pa so: CBC, CTR, OCB, CCM, GCM itd.

3.3.4 Asimetrična kriptografija

Asimetrična kriptografija ali kriptografija javnega ključa (angl. asymmetric encryption ali public key cryptography) je kriptografski sistem, ki za razliko od simetrične kriptografije uporablja dva različna ključa [59]. Prvi je javni ključ (angl. public key), ki je lahko, kot njegovo ime sugerira, javno objavljen in je dostopen vsakomur, ki želi komunicirati z lastnikom ključa. Drugi ključ je zasebni ključ (angl. private key). Ta mora ostati skrivnost in biti poznan samo lastniku ključa, saj na njem sloni varnost sistema. Iz javnega ključa ni mogoče pridobiti zasebnega ključa oz. sklepati o njem. Za šifriranje se uporabi naslovnikov javni ključ. Nastalo šifrirano sporočilo je mogoče dešifrirati samo z naslovnikovim zasebnim ključem. Šifrirana sporočila lahko naslovniku pošilja vsakdo, ki ima njegov javni ključ, in kot je bilo omenjeno, je javni ključ lahko dostopen vsakomur. Če želi entiteta, ki je prejela sporočilo, šifrirati odgovor, mora uporabiti javni ključ naslovnika, ki je bil ob prejšnjem sporočilu pošiljatelj. Ta lahko odgovor dešifrira z uporabo lastnega zasebnega ključa. Preprost diagram uporabe ključev za namene šifriranja in dešifriranja je prikazan na naslednji sliki (Slika 3.3).



Slika 3.3: Postopek asimetričnega šifriranja.

Diffie-Hellmanov algoritem za vzpostavitev ključev je bil prvi primer asimetričnega algoritma, vendar ne omogoča šifriranja ali digitalnega podpisovanja [59]. Diffie-Hellmanov algoritem je namenjen samo vzpostavitvi skupne skrivnosti med dvema entitetama. Med asimetrične algoritme spada, ker vključuje javne in zasebne vrednosti oz. ključe (čeprav jih ni mogoče uporabiti tako, kot je bilo opisano in predstavljeno na sliki). Drugi dobro poznani asimetrični algoritmi so: RSA (Rivest–Shamir–Adleman) [61], ElGamal [62] in kriptografija eliptičnih krivulj – KEK (angl. Eliptic Curve Cryptography – ECC).

Predstavljeno delovanje asimetričnih šifer nima enakih težav z distribucijo ključev, kot jih ima simetrično šifriranje, saj se javni ključ lahko pošlje preko javnega kanala in prisluškovanje tej komunikaciji ne ogrozi varnosti kriptosistema [59]. V asimetrični kriptografiji je število hranjenih ključev zmanjšano. Dovolj je že, če vsaka entiteta hrani samo svoj par ključev. Če ji želi kdor koli drug poslati šifrirano sporočilo, lahko najprej od nje zahteva javni ključ in nato z njim šifrira nadaljnjo komunikacijo. V simetrični kriptografiji to ni mogoče in mora vsaka entiteta hraniti ključ za komunikacijo z vsako drugo entiteto. Pomanjkljivost asimetrične kriptografije je predvsem njena matematična zahtevnost in posledična počasnost delovanja. Zato se asimetrična kriptografija primarno uporablja samo za vzpostavitev simetričnega ključa, s katerim se zatem šifrira prenos podatkov. Druga pomanjkljivost, ki je izrazita predvsem v omrežjih s pomnilniško omejenimi napravami, kjer ni veliko vozlišč (kot je TSO), je znatno večja velikost asimetričnih ključev. V naslednji tabeli (Tabela 3.1) je predstavljena velikost simetričnih in asimetričnih ključev, ki zagotavljajo primerljivo raven varnosti. Iz tabele lahko razberemo, da če bi želeli z algoritmom RSA vzpostaviti 128-biten AES-ključ (kar sta danes priporočena velikost simetričnega ključa in simetričen šifrirni algoritem), bi za to, da ohranimo enako raven varnosti med prenosom ključa (šifriran z RSA) in bodočimi šifriranimi podatki (šifrirani z AES), morali uporabiti 3072-biten asimetrični par ključev. Namesto tega para ključev bi lahko na vozlišču hranili 24 128-bitnih simetričnih ključev. KEK se razlikuje od tipičnih asimetričnih šifer, kot sta RSA in Diffie-Hellmanov algoritem, saj zagotavlja enako raven varnosti ob veliko manjši velikosti ključev (čeprav so ti še vedno dvakrat večji kot primerljivi simetrični ključi). Druga dobra lastnost KEK pred tradicionalnimi asimetričnimi šiframi je manjša računska zahtevnost (čeprav je ta ponovno veliko večja kot pri simetričnih šifrah). Pomanjkljivosti KEK sta predvsem zahtevnejša implementacija in osnovanost na matematičnih načelih, ki so, napram tistim v RSA ali Diffie-Hellmanovemu algoritmu, kompleksnejša [63]. Relativna novost algoritmov predstavlja tudi možnost še neznanih varnostnih pomanjkljivosti. Uporaba KEK je bila in tudi v neki meri še vedno je omejena zaradi patentov, ki se navezujejo na njeno delovanje [64]. Ne glede na te pomanjkljivosti KEK počasi pridobiva številčnost v uporabi, predvsem na področjih s pretežno omejenimi napravami, kot je IoT, kjer je učinkovitost algoritmov toliko bolj pomembna [65].

Tabela 3.1: Primerjava velikosti ključev simetričnih in asimetričnih šifer ob enakovredni ravni varnosti [66].

Velikost simetričnih ključev	**Velikost ključev KEK**	**Velikost ključev RSA in Diffie-Hellman**
80 bitov	160 bitov	1024 bitov
112 bitov	224 bitov	2048 bitov
128 bitov	256 bitov	3072 bitov
192 bitov	384 bitov	7680 bitov
256 bitov	521 bitov	15360 bitov

Asimetrična kriptografija je poleg šifriranja uporabna še za namene digitalnega podpisovanja (angl. digital signature) [59]. Digitalni podpis je proces, ki veže identiteto pošiljatelja na sporočilo in onemogoči ponarejanje ali spreminjanje sporočila. Zagotavlja overjanje pošiljatelja, celovitost sporočila in njegovo nezanikanje. Nezanikanje je lastnost, ki preprečuje, da bi podpis ustvaril kdor koli drug kot lastnik podpisa, torej pošiljatelj ne more zanikati, da je on poslal sporočilo (ne da je bil razkrit njegov zasebni ključ). Digitalno podpisovanje je zelo podobno šifriranju z asimetrično šifro. Digitalni podpis se ustvari, tako da se podatki šifrirajo s pošiljateljevim zasebnim ključem. Ustvarjeni podpis se pripne sporočilu in pošlje naslovniku. Ta ob prejetju dešifrira priloženi podpis s pošiljateljevim javnim ključem. Če je rezultat enak podatkom v sporočilu, je prejemnik lahko prepričan, da podatki med prenosom niso bili spremenjeni in da je pošiljatelj lahko samo lastnik zasebnega ključa, ki je del para z javnim ključem, s katerim je bil digitalni podpis dešifriran. To je osnovno delovanje digitalnega podpisa, v dejanski uporabi se sporočilo pred šifriranjem z zasebnim ključem vedno pretvori v zgoščeno vrednost in šele nato šifrira. Prejemnik mora zato po dešifriranju z javnim ključem ustvariti zgoščeno vrednost prejetih podatkov, preden lahko te primerja z dešifrirano vrednostjo. Vključitev zgoščevalne funkcije je potrebna iz razlogov učinkovitosti kot tudi varnosti podpisa. Digitalno podpisovanje se torej od asimetričnega šifriranja loči v tem, da se pri digitalnem podpisovanju uporabi pošiljateljev par ključev, kjer se zasebni ključ uporabi za šifriranje in javni za dešifriranje, medtem ko se pri šifriranju podatkov uporabi naslovnikov par ključev in se šifriranje opravi z javnim ključem in dešifriranje z zasebnim ključem. Digitalni podpisi so standardna tehnologija, ki se uporablja povsod, kjer je pomembno, da prejeta sporočila niso bila ponarejena ali spremenjena med prenosom – npr. finančne transakcije in distribucija programske opreme.

Infrastruktura javnih ključev (angl. public key infrastructure – PKI) je skupina ljudi, naprav, programske opreme, pravil, politik in postopkov, ki so potrebni za ustvarjanje, distribucijo, upravljanje, uporabo in preklic digitalnih potrdil [59]. Digitalno potrdilo javnega ključa (angl. public key certificate ali digital ceritficate) je dokazilo o lastništvu javnega ključa. Vsebuje podatke o samem ključu in o lastniku ključa (strukturo določa uporabljen standard, npr. X.509). Del digitalnega potrdila je tudi digitalni podpis omenjenih podatkov. Digitalni podpis ustvari overitelj potrdil (angl. certificate authority), ki je zaupanja vredna entiteta. Če je podpis potrdila veljaven in zaupamo podpisniku (overitelju potrdil), potem smo lahko prepričani, da prejeti javni ključ pripada entiteti, zapisani v digitalnem potrdilu. Infrastruktura javnih ključev torej veže identiteto na javni ključ, s čimer omogoča, da entitete zaupajo identitetam ostalih deležnikov v komunikaciji. Identiteto preveri organ za registracijo (angl. registration authority), pri katerem se poda zahteva za digitalno potrdilo. Organ za registracijo overi osebo ali organizacijo, ki je za potrdilo zaprosila. Nato poda zahtevo overitelju potrdil, ki ustvari par ključev in poskrbi, da se v digitalno potrdilo zapiše identiteta lastnika novega potrdila. Organ za preverjanje veljavnosti potrdil (angl. validation authority) je zadnji sestavni del infrastrukture javnih ključev, ki omogoča preverjanje veljavnosti digitalnih potrdil in je istočasno tudi javni register digitalnih potrdil. Organ za preverjanje veljavnosti potrdil hrani tudi seznam preklicanih digitalnih potrdil, ki niso več veljavna. Potrdila postanejo neveljavna,

ko jim poteče veljavnost, ki je določena ob njegovi izdaji, ali pa ko ga lastnik sam prekliče (npr. če je bil razkrit zasebni ključ).

4 Protokoli vzpostavitve ključa v telesnih senzorskih omrežjih

Namen te disertacije je ustvariti nov protokol za overjanje in dogovor o ključu, ki bo primeren za uporabo v TSO in bo varnejši in/ali učinkovitejši od primerljivih obstoječih protokolov. To poglavje je namenjeno predstavitvi posebnosti protokolov vzpostavitve ključa, primernih za uporabo v TSO, opisu tega, kaj jih razlikuje od tradicionalnih protokolov, zakaj je pomembno, da se uporabljajo namenski protokoli in ne protokoli, ki so bili razviti za podobna omrežja, kot so brezžična senzorska omrežja, predstavili bomo pa tudi klasifikacijo protokolov za vzpostavitev ključa glede na njihovo strukturo. Obstoječe protokole bomo tudi razvrstili glede na klasifikacijo. Pri tem se bomo omejili na protokole, pri katerih komunikacija poteka preko brezžičnih povezav, in na protokole, ki so namenjeni splošni uporabi, kar pomeni, da bomo izključili protokole, ki so omejeni na delovanje znotraj specifičnega prostora (npr. bolniške sobe), so namenjeni zmogljivejšim prenosnim napravam, in protokole, ki zahtevajo specifično vrsto senzorskih naprav za delovanje (npr. protokoli, ki delujejo preko zaznavanja gest [67], kar ni uporabno za naprave, ki niso nameščene na rokah uporabnika). V omrežjih, kjer komunikacija poteka brezžično po zraku oziroma etru, je potrebno komunikacijo zaščititi, sicer ji lahko kdo prisluškuje. Za varovanje komunikacije je potrebna uporaba kriptografskega algoritma. Ti za svoje delovanje potrebujejo skrivne ključe. Uporaba varnega načina vzpostavitve ključev med entitetami, ki želijo izmenjevati podatke, je zato ključnega pomena za zagotavljanje varne komunikacije.

Izzivi in omejitve, ki so prisotne v TSO, so veliki meri podedovane od brezžičnih senzorskih omrežij, vendar je nekaj takih, ki so prisotne ali bolj izrazite v TSO:

- **Motnje (angl. Interference)** [68]: Pri komunikaciji v TSO je pomembno, da ne pride do motenj. Te lahko povzročijo težave z uporabnikovim zdrav(ljen)jem ali posredujejo napačno sliko o zdravstvenem stanju zdravstvenim delavcem. Upoštevati je potrebno, da so TSO mobilna omrežja, v katerih prihaja do številnih interakcij med uporabniki (npr. javni promet), kjer nastanejo prekrivanja med posameznimi TSO in posledično je verjetnost motenj visoka [51].
- **Biokompatibilnost, prenosljivost in ustvarjanje toplote** [68, 69]: Senzorske naprave in še posebej vsadki (senzorji, ki se vgradijo v telo) so zelo omejeni glede velikosti, oblike in materialov, iz katerih so narejeni. Naprave morajo biti dovolj majhne in take oblike, da ne ovirajo gibanja uporabnikov ali pri tem povzročajo nelagodje. Narejene morajo biti iz telesu neškodljivih materialov. Istočasno naprave ne smejo proizvajati prekomerne toplote. Povečana temperatura tkiva lahko povzroči bolečine, poškodbe in ustvari okolje, primerno za razvoj bakterij.
- **Energijska učinkovitost** [68]: Zaradi velikosti in okolja, v katerem se senzorji nahajajo, je energetska oskrba omejena. Pogosta potreba po menjavi baterij je

nezaželena, posebej pri vsadkih, kjer menjava baterije zahteva kirurški poseg. Zato je pomembno porabo električne energije zmanjšati, kolikor je le mogoče.

- **Omejen pomnilnik** [69]: Velikost naprav omejuje tudi velikost pomnilnika. Zato mora biti poraba trajnega pomnilnika racionalna.
- **Nizka računska moč** [69]: Tako kot pomnilniški in energetski so tudi računski viri v senzorjih omejeni in njihova prekomerna poraba ni zaželena.
- **Nizka količina komunikacije (angl. Low communication rate)** [69]: Oddajanje sporočil je energetsko najbolj zahtevna operacija. V skladu z omejevanjem porabe energije je zato potrebno izmenjavo sporočil optimizirati oziroma jo povsem odstraniti, kjer je to mogoče. Kjer je mogoče, je dobro komunikacijo nadomestiti z računskimi operacijami (npr. kompresija podatkov pred pošiljanjem). Pokazano je bilo, da je prenos 1 bita tisočkrat bolj energetsko zahteven kot ena 32-bitna računska operacija [70]. To pomeni, da če je mogoče z manj kot tisoč računskimi operacijami zmanjšati velikost sporočila za en sam bit in pri tem ohraniti vse informacije, se to iz vidika porabe energije izplača.
- **Robustnost in odpornost na napake (angl. Robustness and Fault Tolerance)** [68]: Od naprav, ki sestavljajo TSO, se pričakuje dolgotrajno delovanje. Pogosta menjava senzorskih naprav ne more biti dovoljena. Ta lastnost je posebej pomembna za naprave, vgrajene v telo. Pogosti kirurški posegi za namene menjave ali popravila senzorjev so nesprejemljivi.
- **Napakovno razmerje (angl. Error Rate)** [68]: Zaradi pomembnosti podatkov, ki se pošiljajo preko TSO, napake v prenosu niso dovoljene. Zakasnitev, izguba ali modifikacija pomembnih zdravstvenih podatkov je lahko zelo nevarna za uporabnika ali zelo draga za ponudnika zdravstvenih storitev.

Obstoječe rešitve za overjanje in vzpostavitev ključa v žičnih in brezžičnih tradicionalnih omrežjih niso primerne za uporabo v TSO zaradi omejitev, ki so bile predstavljene. Razlika v primerjavi z brezžičnimi senzorskimi omrežji pa razen v zanesljivosti in konstrukciji naprav ni takoj očitna. Zato so tu predstavljene še razlike med obema TSO in brezžičnimi senzorskimi omrežji, ki povzročijo, da je protokol, razvit za overjanje in vzpostavitev ključa v eni izmed obeh omrežij, neprimeren za uporabo v drugem. Te razlike so:

- **Obseg vzpostavitve ključa** [31]: Brezžična senzorska omrežja imajo veliko število vozlišč, ki sestavljajo omrežje, zato se v takšnih omrežjih za namene izmenjave ključev pogosto uporabijo bazeni ključev in verige ključev, ki pa niso primerna rešitev v TSO, kjer je število vozlišč veliko manjše. Takšne rešitve so tudi dokaj pomnilniško potratne, ker zahtevajo hranjenje večjega števila ključev.
- **Različni merjeni podatki**: Čeprav vrsta podatkov, ki jih senzorji zajemajo, tipično ne vpliva na varnostne protokole, se to spremeni, če želimo te podatke dejansko uporabiti za namene ustvarjanja ali dogovora o ključu. Zato ker brezžična senzorska omrežja zbirajo podatke iz okolja, ki je skupno tudi napadalcu, so takšni podatki, četudi imajo nekateri dovolj veliko entropijo, tipično neprimerni za uporabo pri overjanju ali dogovoru o ključu [31]. Po drugi strani imajo podatki, ki jih merijo senzorji v TSO,

tipično visoko entropijo, zaradi česar so primerni za gradnjo ključev in so zajeti iz okolja (uporabnikovega telesa), do katerega napadalec zelo težko na neopazen način pridobi dostop.

- **Fizična dostopnost naprav oziroma shranjenih ključev** [31]: Brezžična senzorska omrežja so tipično uporabljena v okoljih, kjer ni nadzora nad fizičnim dostopom do teh naprav. Zaradi želje po čim bolj poceni napravah je tudi fizična varnost naprav zelo okrnjena. Posledično je za napadalca relativno preprosto dostopati do okolja, v katerem naprave delujejo, jih odtujiti in iz pomnilnika same naprave pridobiti uporabljene ključe. Vozlišča TSO so distribuirana na telesu uporabnika, kjer je za napadalca težko fizično dostopati do naprav. Problematika razkritega ključa preko kompromitirane naprave oziroma vprašanje, kako zmanjšati vpliv takšnega napada, je zato veliko bolj pomembno v brezžičnih senzorskih omrežjih.
- **Razlika v dostopni količini energije**: Naprave v brezžičnih senzorskih omrežjih so omejene z viri, ki jih imajo na razpolago, vendar to še toliko bolj velja za senzorske naprave v TSO. Zato da lahko imajo naprave čim daljšo življenjsko dobo, morajo biti protokoli za overjanje in vzpostavitev ključa še toliko bolj učinkoviti pri izrabi energije, kot so protokoli v brezžičnih senzorskih omrežjih [31]. Poleg tega da so naprave v TSO fizično manjše in imajo posledično manjše kapacitete električne energije, je lahko njihova dolgoživost bolj pomembna, predvsem v primeru, ko gre za v telo vgrajene naprave. Po drugi strani lahko iztrošene naprave v brezžičnih senzorskih omrežjih nadomestimo z novimi napravami, ne da bi prejšnje odstranili.
- **Fizični dostop do vozlišč**: V tretji točki je bilo omenjeno, da je fizični dostop do naprav v brezžičnih senzorskih omrežjih nenadzorovan in posledično lahko kdor koli dostopa do njih, vendar je istočasno fizična odstranitev oziroma zamenjava vseh vozlišč zaradi števila naprav in geografske razpršenosti ter morebitne nedostopnosti praktično nemogoča [71]. Zato se, kot je bilo omenjeno v prejšnji točki, naprave v takšnih okoljih tipično ne zamenjujejo, temveč se zgolj dodajo nove. Teh težav v TSO ni. Čeprav je odstranitev ali menjava naprav nezaželena (predvsem za vgrajene naprave), je mogoča. Vsekakor pa ni zaželeno dodajanje novih naprav v TSO brez odstranitve starih.
- **Disperzija vozlišč**: Vozlišča so v TSO nameščena veliko bližje eno drugemu in na relativno majhnem območju. To pomeni, da so lahko vsa vozlišča v komunikacijskem dosegu in so pogosto povezana v topologijo zvezde [72]. To je v brezžičnih senzorskih omrežjih veliko bolj redko, kar pomeni, da je med senzorsko napravo in bazno napravo potrebnih več posrednikov in posledično morajo biti temu prilagojeni tudi protokoli za overjanje in vzpostavitev ključa [71].

Poleg upoštevanja omejitev, ki so prisotne v TSO, je pomembno, da protokoli za overjanje in dogovor o ključih, primerni za delovanje v takšnem omrežju, izpolnjujejo tudi naslednje zahteve [6, 51, 73]:

- **Overjanje vozlišč (angl. Node authentication)**: Vozlišče overi istovetnost drugega vozlišča, s katerim komunicira, oziroma vozlišči overita eno drugo v primeru medsebojne overitve. To omogoča porazdeljen način overjanja, ki nima kritične točke

odpovedi (angl. single point of failure), ker lahko večje število vozlišč overi vsako posamezno vozlišče. Omogoča tudi identifikacijo problematičnih, potencialno zaupanja nevrednih vozlišč.

- **Odpornost (angl. Resilience)**: Pomeni odpornost protokola vzpostavitve ključa na fizični napad odtujitve vozlišča ali izgubo naprave in posledično razkritje skrivnih vrednosti, hranjenih na vozlišču. Odpornost pove, v kakšni meri takšno razkritje ogroža varnost preostalih vozlišč v omrežju. Pomembno je, da odtujitev enega vozlišča ne razkrije varovane komunikacije ostalih naprav v omrežju. Težave z odpornostjo so prisotne predvsem v protokolih s predporazdeljenimi skrivnostmi.
- **Razširljivost (angl. Scalability)**: Pomeni sposobnost protokola, da se velikost omrežja (ob dodajanju ali odvzemanju naprav iz omrežja) lahko spreminja brez ogrožanja varnosti omrežja. Težave z doseganjem razširljivosti imajo predvsem protokoli s predporazdeljenimi skrivnostmi, kjer dodajanje nove naprave v omrežje vključuje zaupanja vredno tretjo entiteto, ki mora na novo napravo in potencialno na naprave, s katerimi se bo novo vozlišče povezovalo, naložiti nove (predporazdeljene) vrednosti. Slaba razširljivost protokola za vzpostavitev ključa lahko povzroči tudi dodatne režijske stroške in začasen izpad omrežja. Lastnost omrežja, da prosto vključuje in izključuje naprave v omrežju, je dodatno pomembna v TSO zaradi dinamičnega spreminjanja topologije omrežja. Protokoli s funkcionalnostjo priklopi in uporabljaj imajo praviloma dobro razširljivost.
- **Procesna učinkovitost**: Procesna moč, potrebna za overjanje in dogovor o ključih, mora biti karseda majhna. Izvajanje procesno zahtevnih operacij na senzorskih napravah TSO ni zaželeno [74].
- **Komunikacijska učinkovitost**: Pošiljanje podatkov je energetsko zelo zahtevna operacija. Zato je treba biti pri senzorskih napravah, ki imajo omejene zaloge energije, pozoren in stremeti k čim manjšemu številu in velikosti poslanih in prejetih sporočil.
- **Pomnilniška učinkovitost**: Tako kot vsi drugi viri je tudi pomnilnik omejen na senzorskih vozliščih. Zato je za protokol za dogovor o ključu pomembno, da porabi čim manj pomnilnika, ki bo tako lahko uporabljen za druge naloge vozlišča.
- **Energetska učinkovitost**: Vse že omenjene omejitve izrabe virov stremijo k znižanju porabe energije, ki je zelo omejena. Za zagotavljanje dolge življenjske dobe senzorjev je potrebno energetsko zahtevnost znižati na minimum.
- **Priključi in uporabljaj (angl. Plug and play)**: Pomeni sposobnost protokola za dogovor o ključu, da algoritem sam generira in se dogovori o ključu brez človeškega posredovanja. To je dodatna lastnost, ki ni absolutno zahtevana, vendar predstavlja prednost protokolov, ki jo izpolnjujejo. To lastnost, kot bo predstavljeno v nadaljevanju, izpolnjujejo predvsem protokoli, osnovani na fizioloških signalih, ki lahko te signale uporabijo za ustvarjanje ključev in overjanje naprav brez potrebe po predporazdeljenih skrivnostih [6].

Raziskave na področju varovanja komunikacije v TSO se delijo glede na del omrežja (Slika 2.2), v katerem delujejo. Prvi del raziskav v literaturi se ukvarja z vzpostavitvijo varne komunikacije med glavnimi entitetami v TSO. Te so:

- uporabnik (osebni strežnik),
- zdravstveni sistem (podatkovna shramba),
- uporabniki zbranih podatkov (zdravstveni delavci),
- in druge (npr. center za generiranje ključev ali zaupanja vredne entitete).

To je večinoma del omrežja, ki smo ga v poglavju 2.2.1 opredelili kot zunanji TSO. Drugi del raziskav se osredotoča na notranji TSO – komunikacijo s senzorskimi napravami.

Vse naštete omejitve in zahteve TSO ter protokolov, ki v njih delujejo, so specifične za to okolje zaradi kombinacije senzorskih naprav, okolja, v katerem delujejo (telo uporabnika), in podatkov, ki se v omrežju pretakajo (zdravstveni podatki so zahtevni za zaščito in upravljanje, ker so osebne narave in ker so lahko kritični za uporabnikovo preživetje). Doktorska disertacija se osredotoča na protokole overjanja in dogovora o ključu, razvite za delo v tem okolju, kjer so zaradi vrste posredovanih podatkov in strojnih omejitev v tem delu omrežja za vzpostavitev varne komunikacije zahtevane nove rešitve. Ko komunikacija preide na zmogljivejše naprave, se izziv zagotavljanja varnega prenosa podatkov zmanjša oziroma ga je mogoče rešiti z že obstoječimi varnostnimi mehanizmi. To ne pomeni, da zunanji TSO ni zanimiv za raziskovanje, vendar se v tem delu omrežja raziskave tipično osredotočajo na drugo problematiko. Izzivi v zunanjem TSO so predvsem dodeljevanje in upravljanje s pravicami dostopa (angl. access control). Cilj disertacije je razviti protokol za overjanje in dogovor o ključu, primeren za delovanje na senzorskih vozliščih TSO. Zato iz pregleda in primerjave obstoječih protokolov izključimo vse takšne, ki delujejo izključno v vmesnem ali zunanjem TSO.

4.1 Pregled varnostnih zahtev

Za zagotavljanje varne komunikacije je potrebno zadostiti določenim varnostnim zahtevam. Zahteve za varno komunikacijo, ki so naštete spodaj, je mogoče izpolniti z uporabo varne vzpostavitve ključev med napravami. Iz tega razloga je vzpostavitev ključa najpomembnejši del zagotavljanja varne komunikacije. Če je ključ za varovanje prenosa uspešno in varno razdeljen med deležnike, potem ga poznajo samo legitimne entitete in lahko samo one šifrirajo podatke, ki se bodo uspešno dešifrirali pri naslovniku. Zato, da je TSO varno, je potrebno izpolniti naslednje varnostne zahteve:

- **Zaupnost podatkov (angl. data confidentiality)** [69]: Podatki, ki se prenašajo po TSO, so osebni zdravstveni podatki, zato je v interesu porabnika kot tudi samega ponudnika storitev, preprečiti nepooblaščen dostop do teh podatkov. Zaupnost podatkov je tudi med prenosom, ko so ti najbolj dovzetni za razkritje oziroma odtujitev, varovana s pomočjo šifriranja.

- **Overjanje vozlišča (angl. node authenticity)** [69]: Pomeni zmožnost prejemnika sporočila, da overi in se s tem prepriča, da je sporočilo prišlo od navedenega pošiljatelja. Brez te lastnosti bi se lahko vsaka entiteta lažno izdajala za legitimno vozlišče v omrežju in na takšen način pridobila dostop do omrežja.
- **Obojestransko overjanje (angl. mutual authentication)** [75]: Pomeni nadgradnjo overjanja vozlišča, kjer pošiljatelj in prejemnik overita en drugega. Obojestransko overjanje je glavno orodje za preprečevanje napadov s posrednikom.
- **Celovitost podatkov (angl. data integrity)** [69]: Podatke v prenosu je mogoče spremeniti na tak način, da so še vedno zaupni (napadalec ne razbere vsebine sporočila in to se še vedno pravilno dešifrira) in jih prejemnik uspešno overi. To lahko prinese podobne posledice kot uspešno lažno izdajanje za entiteto z dostopom. Celovitost podatkov je zmožnost preprečevanja sprememb podatkov (v primeru vzpostavitve ključa so to sporočila v komunikaciji) oziroma, bolj tipično, zmožnost zaznavanja sprememb v podatkih.
- **Neponaredljivost (angl. unforgeability)** [76]: Zagotavlja, da v omrežje ni mogoče vključiti lažnega prehoda (angl. gateway), ki ga v TSO imenujemo osebni strežnik ali bazna postaja. Takšna naprava zbira podatke, pridobljene v senzorskih omrežjih, in jih posreduje v širše omrežje (zdravstvenemu centru). Protokoli z neponaredljivostjo so odporni na napade s ponarejeno bazno postajo.
- **Nepovezljivost** ali **nesposobnost sledenja (angl. unlinkability** ali **untraceability)** [77]: Nepovezljivost sej ali nesposobnost sledenja uporabniku je strožja oblika anonimnosti pošiljatelja [78, 79]. Anonimnost zahteva, da prisluškovalci iz sporočil ne morejo razbrati identitete pošiljatelja. Nepovezljivost je podobna lastnost, vendar zahtevnejša za realizacijo, ker zahteva, da je iz sporočil nemogoče razbrati, ali izhajajo iz istega vira. Tudi če je komunikacija varovana in so vsa sporočila šifrirana, napadalec ne sme biti sposoben ustvariti povezave med sporočili in pošiljateljem. Z drugimi besedami, napadalec iz sporočil ne more razbrati, ali ta pripadajo istemu pošiljatelju ali več različnim. Nepovezljivost preprečuje napade sledenja.
- **Prihodnja varnost (angl. forward secrecy)** in **pretekla varnost (angl. backward secrecy)** [80]: Prihodnja varnost ali poudarjena zaupnost (angl. perfect forward secrecy) je lastnost sistema, da preprečuje, da se ob razkritju trajnega ključa razkrijejo tudi predhodno uporabljeni sejni ključi. Zato protokoli, ki vzpostavijo ključ s transportom sejnega ključa, šifriranega s trajnim ključem, ne morejo doseči prihodnje varnosti. Prihodnja varnost zagotavlja, da vozlišča, ki se priključijo omrežju, niso sposobna dešifrirati sporočil, ki so bila poslana pred njihovo priključitvijo v omrežje. Prihodnja varnost je opisana kot lastnost sistema, ki ustvari naključen nedeterministični ključ za vsako sejo, tako da če je trajni ali sejni ključ iz kakršnega koli razloga razkrit, ostanejo vse predhodne seje zaupne. Protokol zagotavlja delno prihodnjo varnost (angl. partial forward secrecy), če odkritje trajnih ključev specifičnih deležnikov ne razkrije sejnih ključev predhodne komunikacije (uporabno v primeru različnih vlog deležnikov; npr. odjemalec – strežnik) [81]. Šibka prihodnja varnost

(angl. weak forward secrecy) zagotavlja varnost vseh sejnih ključev, uporabljenih pred razkritjem trajnega ali trenutnega sejnega ključa, za vse seje, v katere napadalec ni aktivno posegal [82]. Pretekla varnost je zelo podobna lastnost, le da preprečuje odkrivanje sejnih ključev prihodnje komunikacije – odstranjenim vozliščem preprečuje dešifriranje sporočil oziroma razkritje ključev, ki so bili uporabljeni po njihovi izključitvi iz omrežja.

- **Razširljivost (angl. scalability)** [80]: Razširljivost ni nujno varnostni parameter, vendar varen protokol mora tipično omogočati spremembe v številu naprav v omrežju. Brez razširljivosti se lahko raven varnosti zmanjša ob dodajanju ali odvzemanju vozlišč iz omrežja.
- **Svežina (angl. freshness)** [19]: Svežina sporočil je lastnost, ki zagotavlja, da lahko prejemnik razlikuje med svežimi in starimi sporočili. Protokoli s to lastnostjo ne bodo dovzetni na napad s ponavljanjem, saj bodo ponovljena (stara) sporočila prepoznana in zavrnjena. Svežina sporočil se najpogosteje doseže z uporabo časovnih žigov ali enkratnih vrednosti. Zagotavljanje celovitosti sporočil mora vključevati tudi časovni žig ali enkratno vrednost, sicer lahko te vrednosti napadalec prosto spreminja.
- **Odpornost na napade**: Pomembna varnostna lastnost vseh protokolov je tudi njihova odpornost na napade. Protokoli morajo biti odporni na napade, ki bodo predstavljeni v naslednjem poglavju.

4.2 Pregled napadov na protokole

Napadi in grožnje v TSO so razdeljeni na pasivne in aktivne. Pasivno zbiranje informacij oziroma prisluškovanje [6, 32] je preprostejše in tipično manj škodljivo od aktivnih napadov [83]. Pasivni napad ne spreminja podatkov, ki se prenašajo, medtem ko aktivni napad spreminja prestreženo komunikacijo z namenom vplivanja na njeno varnost [83]. Aktivni napadi pogosto vključujejo prisluškovanje. Tukaj so zbrani najpogostejši in najpomembnejši napadi na TSO:

- **Napad prisluškovanja (angl. eavesdropping attack)** [84]: Ker je komunikacija v TSO brezžična in se tipično pošilja preko zraka, lahko kdor koli prisluškuje izmenjanim sporočilom. Cilj prisluškovanja je izvedeti vsebino komunikacije ali odkriti pomembne informacije, skrite v sporočilih, tipično z obdelavo velikega števila prestreženih sporočil. Ker je prisluškovanje tako preprosto in ker se v TSO pošiljajo osebni podatki, katerih varovanje je tudi v določeni meri zakonsko opredeljeno, je varovanje pred prisluškovanjem toliko bolj pomembno. Za preprečevanje prisluškovanja je potrebna uporaba šifriranja. Podatkovni prenos se tipično šifrira s simetričnimi šiframi in ob uporabi sejnih ključev, ki morajo biti pogosto menjani. Prisluškovanje je edina oblika pasivnega napada v tem seznamu.
- **Ponarejanje sporočila (angl. message corruption)** [6, 32]: Stopnjevanje prisluškovanja vodi v napad, kjer napadalec ne želi le izkoristiti prestreženih

informacij, temveč izbrisati ali spremeniti posredovane podatke z namenom vplivati na neki rezultat komunikacije. Ukrepi za zaščito so enaki kot pri preprečevanju pasivnega prisluškovanja. V TSO je ključnega pomena, da uporabnikovi zdravstveni podatki med prenosom ostanejo celoviti (se ne spremenijo), sicer ima lahko to tudi usodne posledice za uporabnika.

- **Napad poosebljanja (angl. impersonation attack)** [32]: Omogoča napadalcu, da se vključi v omrežje in predstavi kot pooblaščena naprava. Napadalec pridobi zasebne identifikacijske podatke entitete in se z njimi izdaja za legitimno entiteto v omrežju. Napad je uspešen, če napadalec pridobi enake pravice kot legitimno vozlišče. Pred napadi poosebljanja varuje overjanje vozlišč.
- **Napad s ponavljanjem (angl. replay attack)** [6, 77]: Napadalec zajame poslano sporočilo in ga v določenem trenutku ponovno pošlje prejemniku. Ker gre za veljavno sporočilo, ki je zaščiteno z ustreznim ključem, in je pošiljatelj ustrezno overjen, je lahko takšno sporočilo brez ustreznih protiukrepov sprejeto kot veljavno. Napadalec lahko s takšnimi sporočili doseže zlonamerne cilje, npr.: Oseba A plača neko storitev osebi B s tem, da pošlje sporočilo banki o prenakazilu denarja. Oseba B lahko prestreže poslano sporočilo in ga kadar koli v prihodnosti ponovi in ponovno prejme plačilo. Ker gre v primeru ponovljenih sporočil za veljavna sporočila, ki jih mora prejemnik obdelati, lahko napad s ponavljanjem napadalec uporabi tudi kot način izčrpanja omejenih virov, ki so na razpolago napravam. To stori tako, da pošlje ogromno število ponovljenih sporočil in s tem prisili naslovnika v nepotrebno obdelavo podatkov in posledično izrabo zelo omejene zaloge energije. Zato je pomembno, da je vsako sporočilo varovano na način, ki ne omogoča, da bi lahko bilo zajeto in poslano kot veljavno sporočilo kadarkoli v prihodnosti. Za preprečevanje takšnih napadov sta potrebna overjanje in svežina sporočil.
- **Napad vrinjenega napadalca (angl. Man in The Middle attack – MiTM)** [77]: Napadalec je zmožen prestrezati sporočila in jih posredovati namenjenemu prejemniku, ne da bi entiteti v komunikaciji to opazili. To je eden najmočnejših (in najpogosteje omenjanih) napadov, ker omogoča prisluškovanje in spreminjanje izmenjanih podatkov v realnem času. Napad posrednika (angl. relay attack) je oblika napada MiTM, pri kateri napadalec sproži komunikacijo med dvema entitetama [60].
- **Napad ugibanja gesla s povezavo (angl. on-line guessing attack)** in **napad ugibanja gesla brez povezave (angl. off-line guessing attack)** [77]: Ta napada sta možna le na sistemih, ki za svoje delovanje uporabljajo gesla. Pri napadu ugibanja gesla s povezavo se napadalec poskuša prijaviti na strežnik z ugibanjem gesla. Napad ugibanja gesla brez povezave omogoča napadalcu, da preveri pravilnost ugibanega gesla brez komunikacije s strežnikom. Ta napad zahteva, da napadalec najprej zbere vse potrebne informacije o postopku prikrivanja gesla. Ko je ta znan, lahko napadalec preverja pravilnost ugibanih gesel glede na zajeto skrito geslo brez komunikacije s strežnikom (ker lahko sam pretvori ugibano geslo v skrito obliko in nato samo primerja z zajeto vrednostjo). Varovanje pred napadi ugibanja gesla s povezavo je tipično skupek

pravil oziroma omejitev v procesu preverjanja gesla (npr. omejeno število poizkusov vnosa gesla), ki se v celoti izvajajo in so odvisne od strežnika, zato varovanje pred takšnim napadom ni del samega varnostnega protokola. Napad ugibanja gesla brez povezave ni omejen s pravili strežnika in je posledično veliko hitrejši in zahtevnejši za preprečitev. V znanstveni literaturi se pogosto obe obliki napadov združita v enotno poimenovanje (napad ugibanja gesla), z razumevanjem, da se naslavlja predvsem napad ugibanja gesla brez povezave, ker ta predstavlja večjo grožnjo.

- **Napad za zavrnitev storitve (angl. denial of service – DoS)** [6, 85]: Napad je namenjen onemogočanju dostopa do storitve ali omrežnega vira. Deluje tako, da poplavi tarčo napada s tolikšno količino lažnega prometa, da je ta nezmožna obdelati vse prispele komunikacije in posledično nedosegljiva za legitimne uporabnike. Poleg preprečitve pravilnega delovanja tak napad vpliva tudi na porabo energije napadenih naprav. Ščitenje pred takšnimi napadi je zelo zahtevno in je do neke mere celo nemogoče. Glavni način zaščite je razpoznavanje legitimne komunikacije in zavračanje vseh ostalih povezav. Napad za zavrnitev storitve je zelo učinkovit v omrežjih z omejeno količino virov, kot je TSO, ker tudi zaščita pred napadom vključuje neko izrabo virov, ki so že tako zelo omejeni. Protokoli, namenjeni varovanju komunikacije v TSO, tipično ne vključujejo preprečevanja napadov za zavrnitev storitve in raziskovalci tega tudi ne štejejo kot zahtevan del protokolov (npr. [74]).
- **Napad zajetja vozlišča** ali **kompromitirano vozlišče (angl. node capture attack** ali **node-compromising attack)** [6, 84, 86] in **napad s klonom (angl. clone attack)** [87]: Ker je zaradi kombinacije tehnoloških in stroškovnih vidikov praktično nemogoče ustvariti senzorske naprave, ki bodo odporne na nedovoljeno dostopanje, je pri oblikovanju varnostnih protokolov potrebno upoštevati, da lahko napadalec, ki zajame napravo, pridobi vse podatke, ki so shranjeni na njej (vključno s skrivnimi vrednostmi), in jih uporabi za pridobitev nepooblaščenega dostopa v omrežje. V TSO je tveganje odtujitve vozlišča manjše, saj se naprave ves čas nahajajo v kontaktu z uporabnikom in je zato kraja, ne da bi jo uporabnik opazil, skoraj nemogoča. Ne glede na to je pomembno, da protokoli omogočajo preklic ključev in redno spreminjanje ključev, tako da v primeru odtujitve naprave in skritega ključa napadalec ne more razbrati predhodne in prihodnje komunikacije, kar se navezuje tudi na prihodnjo in preteklo varnost. Pomembno je tudi, da odkritje skrivnih vrednosti ene naprave ne ogrozi varnosti komunikacije drugih naprav. Napad s klonom je podoben, saj je tudi za ta napad potrebno odtujiti vozlišče v omrežju. Napadalec prepiše celotno vsebino vozlišča na lastno napravo. Nastali klon, ki je pod nadzorom napadalca, se zatem poizkuša vključiti v omrežje.
- **Napad sledenja (angl. tracking attack)** [86]: Pri napadu sledenja lahko napadalec prosto prisluškuje vsej komunikaciji v omrežju. Če lahko na podlagi tega napadalec določi, katero sporočilo prihaja od katerega vozlišča ali specifičnega TSO (sporočilo pripada določenemu uporabniku), potem se napad šteje kot uspešen. Napad je uspešen tudi, če je mogoče pokazati, da sporočila pripadajo isti entiteti, čeprav trenutno identiteta te entitete ni znana. Napad je relevanten, ker že sama informacija o tem, kdo

komunicira s kom in ob katerem času, lahko izda veliko osebnih podatkov o uporabniku.

- **Napad odsevanja (angl. reflection attack)** [60]: Pomeni napad na obliko overjanja poziv-odziv (angl. challenge-response). Uporabiti ga je mogoče v sistemih, kjer se isti poziv-odziv uporabi za overjanje obeh strani v komunikaciji. Napadalec lahko pravilno odgovori na poziv, tako da pošlje identičen poziv entiteti, od katere je prejel poziv. Ker se uporablja isti poziv-odziv, bo pobudnik overjanja napadalcu sam poslal pravilen odziv, ki ga bo zatem napadalec uporabil kot odziv na prvoten poziv in se s tem uspešno overil.
- **Napad z ujemanjem (angl. matching attack)** [86]: Napadalec ustvari veliko število javnih ključev in z njimi šifrira možna sporočila. Če pri tem najde rezultat, ki je enak kateremu od predhodno poslanih šifriranih sporočil, je odkril javni ključ. Ta napad je uporaben, ko je število vseh možnih vrednosti, ki se šifrirajo, relativno omejeno.
- **Napad zarote (angl. collusion attack)** [88]: Za ta napad napadalec potrebuje skrite vrednosti drugih vozlišč. Napad je uspešen, če lahko na podlagi teh podatkov napadalec ustvari ključ vozlišča v omrežju, za katerega ni poznal skritih vrednosti. Začetne informacije o skritih vrednostih lahko napadalec pridobi od zlonamernih uporabnikov, ki prispevajo svoje lastne skrite vrednosti, ali z dostopom do več kompromitiranih vozlišč oziroma s sodelovanjem več napadalcev, kjer je vsak pridobil nekaj skritih vrednosti.
- **Napad poosebljanja s kompromitiranim ključem (angl. key-compromise impersonation attack)** [89]: V primeru, da napadalec pridobi zasebni ključ naprave, je jasno, da lahko s tem ključem pooseblja entiteto, katere zasebni ključ je pridobil. Tega ni mogoče preprečiti v protokolih, ki delujejo na osnovi kriptografije javnega ključa (razen s preklicem certifikata v infrastrukturi javnih ključev). Napad poosebljanja s kompromitiranim ključem pa omogoča tudi poosebljanje v drugo smer – napadalec lahko v komunikaciji z napravo, ki je lastnik kompromitiranega zasebnega ključa, pooseblja druge entitete v omrežju.
- **Napad s ponarejeno bazno postajo (angl. forge base station attack)** [87]: Napadalec se uspešno predstavi v omrežju kot osebni strežnik oziroma privzeti prehod in na tak način zbira podatke od vseh senzorskih vozlišč.
- **Napad desinhronizacije (angl. desynchronization attack)** [90]: Napad desinhronizacije je mogoč, ko je potrebno sinhrono posodabljanje hranjenih vrednosti na ločenih napravah. Potem ko ena naprava posodobi svoje stanje, napadalec prepreči, da bi nova vrednost dosegla drugo napravo, ki zato ne more pravilno posodobiti svojega stanja. Takšni napravi v prihodnosti ne bosta več mogli uspešno vzpostaviti novega ključa.
- **Napad požiralnika (angl. sinkhole attack)** in **selektivno posredovanje (angl. selective forwarding)** [91]: Napadalec poizkuša privabiti čim več prometa (npr. s ponarejeno bazno postajo) na napravo, ki je pod njegovim nadzorom. V primeru selektivnega posredovanja napadalec posreduje le del prejetih sporočil v dostavo,

medtem ko ostala sporočila zavrže. V napadu požiralnika so vsa prejeta poročila zavržena in ta nikoli ne prispejo do ciljne naprave.

- **Napad Sybil (angl. Sybil attack)** [92]: Pogosta oblika obrambe pred različnimi grožnjami je uporaba redundance. Napad Sybil je namenjen izkoriščanju uporabe redundance za pridobitev nesorazmerno velikega vpliva v sistemu. V napadu se ena sama zlonamerna entiteta predstavlja z več identitetami. Primer sistema, ki uporablja redundanco za večanje odpornosti na napade, je sistem, v katerem se zaupanje nove entitete oceni na podlagi glasovanja entitet, ki jih je sistem že sprejel kot zaupanja vredne. Z uporabo napada Sybil zlonamerna entiteta ustvari veliko število identitet in tako večkrat glasuje (lahko tudi zase), dokler sistem ne sprejme entitete kot zaupanja vredne. Napad Sybil je tipičen primer vrinjanja paketov (angl. packet injection).
- **Poplavljanje s hello sporočili (angl. hello flood attack)** [91]: V nekaterih protokolih vozlišča uporabijo pozdravna ali hello sporočila za obveščanje sosednjih vozlišč o svojem obstoju. Vozlišča, ki prejmejo ta sporočila, predvidevajo, da je vozlišče, ki ta sporočila pošilja, v dosegu oddajanja. Napadalec lahko izkoristi takšno delovanje in pošilja takšna sporočila z veliko večjo oddajno močjo in tako zavede vozlišča v mišljenje, da je naprava, ki ta sporočila oddaja, dejansko njihov sosed. Če zatem uspe napadalcu prepričati vozlišča, ki so sprejela ta hello sporočila, da je naprava, ki jih pošilja, dober posrednik za njihovo komunikacijo, in začnejo naprave pošiljati sporočila preko napadalčeve naprave, bodo vsa ta sporočila izgubljena, saj ne bodo nikoli dosegla oddaljene naprave. Takšen napad je lahko uspešen že samo z uporabo ponovljenih sporočil, ki jih je prvotno ustvarilo legitimno vozlišče zunaj dosega napadenih naprav.
- **Napad s črvino (angl. wormhole attack)** [93]: Napadalec prejme sporočila v določeni točki v omrežju. Ta sporočila so zatem poslana preko črvine v drug del omrežja, kjer so ponovno poslana v omrežje. Ta napad omogoča napadalcu izvajanje drugih napadov. Napad s črvino, napad požiralnika, selektivno posredovanje, poplavljanje s hello sporočili in napad Sybil so napadi usmerjanja (angl. routing attacks). Takšne oblike napadov tipično niso učinkovite v TSO, ker so vozlišča tako blizu eno drugemu, da je komunikacija, kjer je potrebnih več skokov, da sporočila prispejo do naslovnika, zelo redka. Zato je v protokolih, ki delujejo v TSO, težko najti pomanjkljivosti, ki bi jih usmerjevalni napadi lahko izkoristili [71].

4.3 Klasifikacija protokolov za vzpostavitev ključa v telesnih senzorskih omrežjih

Zaradi velikega potenciala TSO za izboljšanje zdravstva in zmanjšanje njegovih stroškov ter omejitev TSO je področje vzpostavitve ključa v takšnem omrežju zelo zanimivo za raziskovalce. Novo okolje, v katerem morajo senzorske naprave delovati, in omejeni viri, ki jih imajo pri tem na razpolago, so privedli do novih rešitev in načinov zagotavljanja vzpostavitve ključa v TSO.

Na podlagi teh načinov so se oblikovale različne skupine protokolov, ki delujejo na podlagi podobnih principov. Klasifikacijo protokolov za vzpostavitev ključa na podlagi njihovega delovanja sta predstavila Ali in Khan [6]. V članku sta protokole za vzpostavitev ključa v TSO razdelila v tri skupine: protokoli, ki ne delujejo na podlagi fizioloških vrednosti, protokoli, ki delujejo na podlagi fizioloških vrednosti, in hibridni protokoli.

V skupini protokolov, ki ne delujejo na podlagi fizioloških vrednosti, so, kot že ime nakazuje, protokoli, ki pri svojem delovanju ne uporabljajo vrednosti, pridobljenih iz fizioloških signalov. Večina protokolov v tej skupini je tradicionalnih protokolov, delujočih na podlagi asimetrične kriptografije ali predporazdeljenih ključev. Prednost takšnih protokolov je predvsem majhna količina obdelovanja podatkov, vendar lahko predporazdeljeni ključi zasedejo velik del pomnilnika. V to skupino protokolov so vključeni tudi drugi protokoli, ki za svoje delovanje potrebujejo vrednosti iz okolja (vendar to niso fiziološke vrednosti). Protokoli, ki delujejo na podlagi fizioloških vrednosti, uporabljajo vitalne znake telesa za ustvarjanje skritih ključev. Ker so vse naprave v TSO na istem telesu, lahko nepovezane naprave na podlagi fizioloških signalov, ki so močno korelirani tudi na različnih mestih telesa, ustvarijo enak ključ. To odstrani potrebo po predporazdeljevanjem ključev in zmanjša porabo pomnilnika, vendar zahteva več obdelave podatkov, da se iz zajetih fizioloških signalov ustvari ključ, ki izgleda naključno. Hibridni protokoli so tretja skupina protokolov, v kateri se uporabita oba prejšnja pristopa za vzpostavitev ključa. Hibridne rešitve so najpogosteje sestavljene iz predporazdeljenih skrivnosti, ki so se uporabile skupaj s fiziološkimi vrednostmi za namene vzpostavitve ključa.

Po pregledu obstoječih protokolov, ki so bili predlagani za vzpostavitev ključa v TSO, smo ugotovili, da so tradicionalni načini vzpostavitve ključa zelo različni od protokolov generiranja skritega ključa. Slednji so v svojem delovanju in strukturi veliko bolj podobni protokolom, ki delujejo na podlagi fizioloških vrednosti, zato ni primerno, da se klasificirajo v skupino protokolov, s katerimi imajo manj skupnega. Protokoli vzpostavitve ključa s fiziološkimi vrednostmi in protokoli vzpostavitve ključa z generiranjem skritega ključa za svoje delovanje uporabljajo signale, ki so omejeni samo na zelo majhno področje, medtem ko tradicionalni protokoli vzpostavitve ključa za svoje delovanje ne potrebujejo nobenih podatkov iz okolja, v katerem se nahajajo. Kljub podobnosti pa obstajajo med protokoli vzpostavitve ključa s fiziološkimi vrednostmi in protokoli vzpostavitve ključa z generiranjem skritega ključa tudi določene razlike, po katerih lahko ločimo med obema oblikama vzpostavitve ključa. Prva in najbolj očitna razlika je uporaba fizioloških vrednosti v protokolih vzpostavitve ključa s fiziološkimi vrednostmi. Te vrednosti je mogoče uporabiti samo v TSO oziroma na napravah, ki se nahajajo na živem telesu, medtem ko protokoli vzpostavitve ključa z generiranjem skritega ključa uporabljajo vrednosti signalov, ki so prisotne v neposredni bližini senzorskih naprav in jih je tipično mogoče najti v vsakem okolju. Najpogosteje uporabljena oblika takšnih podatkov so karakteristike komunikacijskega kanala, ki so specifične za vsako povezavo. Protokoli vzpostavitve ključa z generiranjem skritega ključa zato niso primerni za uporabo samo na napravah, ki se nahajajo na telesu, ampak v kakršnemkoli omrežju (npr. brezžičnih senzorskih omrežjih). Druga pomembna razlika med obema skupinama protokolov je v načinu

uporabe pridobljenih vrednosti. Fiziološke vrednosti se v protokolih tipično uporabljajo za omogočanje varnega transporta ključa (ki je lahko generiran na kakršenkoli način), medtem ko se v protokolih vzpostavitve ključa z generiranjem skritega ključa zajete vrednosti tipično uporabijo neodvisno na različnih napravah za dejansko, kot ime nakazuje, generiranje ključa. Zato vpeljemo novo klasifikacijo protokolov za vzpostavitev ključa v TSO, kjer ločimo štiri različne skupine:

- tradicionalni protokoli vzpostavitve ključa,
- protokoli vzpostavitve ključa na osnovi fizioloških podatkov,
- protokoli vzpostavitve ključa z generiranjem skrivnega ključa,
- hibridni protokoli vzpostavitve ključa.

V naslednjih štirih podpoglavjih bo vsaka od teh skupin protokolov podrobneje predstavljena. Izpostavljene bodo tudi razlike, ki so možne med protokoli znotraj iste skupine. V vsaki skupini bodo na kratko predstavljeni oziroma našteti protokoli iz literature, ki spadajo v posamezno skupino. To in naslednje poglavje sta nastali iz pregleda literature za področje vzpostavitve ključa v TSO. Vsi vključeni protokoli ne zagotavljajo overjanja, čeprav je to pogosto prisotno. Preostanek tega poglavja služi tudi kot pregled obstoječe literature za področje protokolov za vzpostavitev ključa, namenjenih uporabi v TSO. Predlagana klasifikacija, pregled obstoječih protokolov in analiza metod ocenjevanja varnosti in učinkovitosti protokolov (preostanek poglavja 4 in poglavje 5) so bili povzeti po objavljenem članku z naslovom *Survey on Security in Intra-Body Area Network Communication* [94] v reviji *Ad Hoc Networks*.

4.3.1 Tradicionalni protokoli vzpostavitve ključa

Skupino teh protokolov smo poimenovali tradicionalni protokoli, ker so najstarejša in istočasno najbolj pogosto uporabljena oblika vzpostavitve ključa. Med tradicionalne protokole vzpostavitve ključa spadajo metode, ki uporabljajo asimetrično kriptografijo in predporazdeljevanje ključa. V veliki večini gre tudi pri uporabi asimetričnih algoritmov za predporazdeljevanje ključa, saj zelo redki protokoli vključujejo mehanizme za deljenje javnih ključev oziroma bi to predstavljajo dodatno breme za senzorske naprave.

Asimetrično šifriranje je računsko veliko bolj zahtevno in glede na uporabo lahko zasede večjo količino pomnilnika za shranjevanje ključev ter lahko potrebuje zaupanja vredne tretje entitete [95]. Ne glede na to je bilo predlaganih nekaj protokolov za vzpostavitev ključa v TSO, ki primarno uporabljajo algoritme, kot sta RSA in ElGamal [96–99].

Čeprav je asimetrično šifriranje v osnovi prezahtevno za uporabo v TSO, obstaja oblika asimetrične kriptografije, ki je veliko bolj pogosto uporabljena v TSO. Kriptografija eliptičnih krivulj – KEK je pomnilniško in računsko manj zahtevna kot klasične asimetrične šifre in posledično veliko bolj primerna za uporabo v TSO [15, 100]. KEK ima primerljivo raven varnosti kot RSA in ElGamal ob uporabi izrazito manjših ključev [84]. Uporaba KEK na manj zmogljivih napravah je bila raziskana [101] in tudi primerjana z algoritmom RSA [102]. Rezultati so še dodatno potrdili prednosti uporabe takšne asimetrične kriptografije. Na

primernost KEK za uporabo v TSO kaže tudi veliko večje število predlaganih protokolov, ki to obliko šifriranja izkoriščajo v svojem delovanju [80, 103–110]. Poleg naštetih protokolov se KEK uporablja tudi v navezi z Diffie-Hellmanovim algoritmom, iz česar nastane Diffie-Hellmanova eliptična krivulja (angl. Elliptic Curve Diffie-Hellman), ki je asimetrični šifrirni sistem, ki deluje kot Diffie-Hellmanova vzpostavitev ključa, vendar za to uporablja KEK. Nekaj protokolov uporabi KEK tudi za šifriranje na podlagi identitete (angl. identity based encryption). Takšni protokoli so predstavljeni v [84, 86, 95, 111–113]. Protokol TinyZKP [87] je protokol z ničelno spoznalnim dokazom (angl. zero-knowledge proof), ki tudi uporablja KEK.

Kljub učinkovitosti KEK v primerjavi s klasičnimi asimetričnimi šiframi je KEK še vedno veliko zahtevnejša oblika šifriranja kot simetrično šifriranje.

Protokoli s predporazdeljenim ključem so druga oblika tradicionalnih protokolov. Takšna oblika protokolov je praviloma najučinkovitejši način vzpostavitve ključa (ko gre za predporazdeljene simetrične ključe), vendar je težko prilagodljiv spremembam v omrežju in spremembe poverilnic (angl. credentials) so zahtevne. Majhna poraba virov je najpomembnejša lastnost v TSO, zato so tudi raziskave o metodah vzpostavitve ključa s predporazdeljenim ključem najpogostejše [19, 20, 72, 75, 85, 90, 114–127]. Nekateri od teh protokolov so namenjeni varovanju komunikacije tudi izven notranjega TSO in nekateri od teh protokolov uporabljajo različne pristope za vzpostavitev varne komunikacije med notranjim in zunanjim TSO. Takšni protokoli so vključeni v pregled literature, ker med drugim omogočajo tudi vzpostavitev ključev za senzorske naprave.

Glavna prednost protokolov s preddistribucijo skrivnega materiala pred protokoli vzpostavitve ključa s fiziološkimi vrednostmi in protokoli vzpostavitve ključa z generiranjem skritega ključa je veliko manj procesiranja, ki je potrebno za vzpostavitev ključa (zbiranje okolijskih vrednosti in transformacija teh vrednosti v naključne vrednosti, ki so primerne za uporabo v kriptografiji, zahteva določena preoblikovanja) [73]. Slabosti predporazdeljenih ključev pa so večja poraba pomnilnika in tipično slabša prilagodljivost protokola pri dodajanju ali odstranjevanju naprav iz omrežja. Protokoli za vzpostavitev ključa v TSO se pogosto označijo kot lahki (angl. lightweight). Takšno poimenovanje je pogosto predvsem pri protokolih s predporazdeljenim ključem, ki za svoje delovanje uporabljajo samo simetrično šifriranje, zgoščevalno funkcijo, operacijo XOR in/ali spajanje. Vse naštete operacije so nezahtevne in posledično primerne za uporabo v TSO.

Med tradicionalnimi protokoli bi radi posebej poudarili tri protokole, ki delujejo na osnovi predporazdeljenih ključev in jih bomo v nadaljevanju disertacije uporabili za primerjavo s protokoloma, razvitima v tej disertaciji.

Abdmeziemov in Tandjaouijev protokol, predstavljen v [122], predlaga nov način transporta ključa, pri katerem se zahtevne operacije asimetrične kriptografije prenesejo iz senzorskih vozlišč, kjer je njihova uporaba nezaželena, na tretje naprave, ki lahko takšne operacije izvajajo. Rešitev omogoča vzpostavitev ključa, ki varuje prenos podatkov med senzorskimi napravami in oddaljenim strežnikom v zdravstvenem centru, ki zbira zdravstvene podatke vseh uporabnikov. Senzorji imajo predporazdeljene podatke o tretjih napravah in ključe, s pomočjo

katerih vzpostavijo varno komunikacijo z njimi. Tretje naprave sodelujejo oziroma pomagajo pri vzpostavitvi ključa med vozliščem in strežnikom. Vozlišče ustvari ključ, ga razdeli na manjše dele in pošlje vsem tretjim napravam, ki so pripravljene pomagati pri vzpostavitvi Ta del komunikacije je varovan s predporazdeljenimi simetričnimi ključi. Tretje naprave se overijo pri strežniku s pomočjo infrastrukture javnih ključev in potem preko varne povezave posredujejo strežniku dele ključa, ki so jih prejele od senzorskega vozlišča. Strežnik zbere dele ključa, ki jih je prejel od različnih tretjih naprav, in jih združi v celoto. Na tak način strežnik pridobi enak ključ, kot ga je ustvarilo vozlišče, ne da bi posredniki vedeli več kot le majhen delček ustvarjenega ključa in brez potrebe po uporabi asimetrične kriptografije na senzorskih napravah. V poglavju 6 bo ta protokol podrobneje predstavljen. Izpostavili bomo tudi njegove pomanjkljivosti in predlagali izboljšave, ki odkrite ranljivosti odpravijo.

Protokola, predstavljena v [90, 123], imata veliko skupnega. Oba sta relativno nova. Oba sta namenjena delovanju v dvonivojski zvezdni topologiji (angl. two-tier star topology), kjer senzorske naprave pošiljajo podatke bazni postaji preko vmesnih vozlišč, ki so tipično nekoliko zmogljivejše naprave, sposobne zajemanja podatkov in posredovanja podatkov drugih manj zmogljivih vozlišč, ki niso v dosegu bazne postaje. Oba protokola uporabljata predporazdelitev skrivnega materiala na vsa vozlišča in bazno postajo, na podlagi katerega se vzpostavi dinamičen sejni ključ, primeren za varovanje nadaljnjega prometa med napravami. Zaradi takšnega delovanja tudi oba protokola spadata med tradicionalne protokole vzpostavitve ključa. Oba protokola sta namenjena dogovoru o ključu, kar pomeni, da je ustvarjeni sejni ključ odvisen od obeh deležnikov. Oba protokola spadata med lahke protokole, saj za svoje delovanje uporabljata samo nezahtevne operacije – zgoščevalne funkcije in operacije XOR. Oba imata podobno strukturo in delovanje obeh je razdeljeno v tri faze. Oba protokola poleg varnostnih lastnosti, ki jih izpolnjujejo drugi protokoli, poudarjata tudi lastnost nepovezljivosti oziroma odpornosti na napade sledenja. V vseh naštetih lastnostih sta podobna tudi protokolu, ki je bil razvit v tej disertaciji (poglavje 7). Avtorji obeh protokolov so njuno delovanje tudi dobro in natančno opisali in analizirali. Iz vseh naštetih razlogov sta primerna, da služita kot osnova oziroma trenuten standard protokolov za dogovor o ključu, primeren za uporabo v TSO. Oba protokola bosta primerjana z novo razvitim protokolom v varnosti in učinkovitosti. Novi protokol bomo primerjali z omenjenima protokoloma in na podlagi tega umestili predlagani protokol v trenutno stanje na področju protokolov overjanja in dogovora o ključu v TSO.

4.3.2 Protokoli vzpostavitve ključa na osnovi fizioloških podatkov

Edinstveno okolje, v katerem delujejo senzorske naprave v TSO, omogoča pridobivanje fizioloških signalov, kar je vodilo k nastanku protokolov za vzpostavitev ključa na osnovi fizioloških podatkov. V takšnih protokolih dve ali več naprav neodvisno meri isti fiziološki signal, ki je unikaten za vsakega uporabnika. Iz teh meritev se po določenem preoblikovanju pridobi vrednost, skupna vsem deležnikom. Takšno delovanje zmanjša število izmenjav med napravami, saj je za vzpostavitev ključa potrebno samo eno sporočilo, ki se lahko pošlje že skupaj s šifriranimi podatki. Takšno delovanje pomaga pri učinkovitosti protokola, saj je

prenos podatkov med napravami energijsko najzahtevnejša operacija. Zmanjša se tudi izraba pomnilnika, saj ni potrebno hraniti trajnega ključa [31]. Pomanjkljivosti takšnih protokolov, sta predvsem potreba senzorskih naprav, da merijo isti signal s pomočjo katerega varujejo vzpostavitev ključev, ter dodatno računsko obdelovanje zajetih vrednosti, ki je potrebno preden so te primerne za varovanje vzpostavitve ključa [31, 128].

Telesa proizvajajo številne fiziološke signale, ki bi se lahko uporabili za namene vzpostavitve ključa: krvni tlak, elektrokardiogram – EKG (angl. electrocardiogram – ECG) (primeri protokolov [77, 129–146]), fotopletizmogram – FPG (angl. photoplethysmogram - PPG) (primeri protokolov [129, 132, 147, 148]), vrednost kisika v krvi (SpO2; angl. blood oxygen level), število krvnih ploščic (angl. blood platelets) itd. Iz v znanstveni literaturi predlaganih protokolov je razvidno, da ti vedno uporabljajo EKG ali FPG. Razlog za to je predvsem preprostejše pridobivanje podatkov za testiranje razvitih protokolov. Večina protokolov je razvitih tako, da jih je mogoče uporabiti s katerim koli fiziološkim signalom z minimalnimi spremembami. Edini pogoj je, da vse naprave, ki želijo vzpostaviti ključ, merijo isti fiziološki signal.

Uporaba simetričnega šifriranja za namene vzpostavitve ključa ima določene pomanjkljivosti. Te se pokažejo predvsem pri odpravljanju posledic odkritega ključa oziroma pri fizični odtujitvi naprav. Kljub visoki varnosti simetričnih kriptosistemov [149] je veliko raziskovalcev mnenja, da je prihodnost protokolov vzpostavitve ključa v uporabi fizioloških podatkov. Ideja za uporabo fizioloških signalov je bila prvič predstavljena leta 2003 v članku [69]. Ta izvirna ideja za uporabo fizioloških signalov je bila kmalu nadgrajena z idejo o uporabi časa med zaporednimi živčnimi impulzi (angl. interpulse interval – IPI), predstavljeno v [15]. Takšna oblika merjenja je primerna predvsem v EKG in FPG. Ker je fiziološke signale mogoče meriti le na telesu, se protokoli vzpostavitve ključa, ki delujejo na osnovi takšnih signalov, uporabljajo praviloma samo v notranjem TSO in na napravah, ki so v stiku s telesom [16].

Fiziološki podatki se v protokolih vzpostavitve ključa praviloma uporabljajo (na način, ki ne razkrije samih fizioloških podatkov) za prikrivanje simetričnega sejnega ključa. Delovanje takšnih protokolov je v osnovi zelo preprosto. Senzorski vozlišči, ki želita vzpostaviti ključ, zajameta meritve istega signala in ga pretvorita v binarni niz. Pošiljatelj zatem ustvari naključni simetrični sejni ključ. S tem ključem že lahko šifrira podatke, ki jih želi poslati in jih pripne sporočilu. Ustvarjeni sejni ključ je zakrit z uporabo binarnega niza, ustvarjenega iz meritev fiziološkega signala. Zakriti ključ se lahko zatem skupaj s šifriranimi podatki pošlje prejemniku. Prejemnik lahko s pomočjo binarnega niza, ustvarjenega iz lastnih meritev istega fiziološkega signala, odkrije zakriti sejni ključ. S tem ključem lahko dešifrira podatke, ki so bili priloženi prejetemu sporočilu. Ta ključ se v nadaljevanju uporablja za šifriranje vse komunikacije, brez potrebe po ponovnem merjenju fizioloških signalov. Fiziološke podatke je treba ponovno meriti šele ob naslednji vzpostavitvi ključa, ki je lahko posledica spremembe v topologiji, zaradi poteka veljavnosti trenutnega sejnega ključa ipd. Eden prvih protokolov vzpostavitve ključa na osnovi fizioloških podatkov [150] vidno sledi predstavljeni metodi uporabe fizioloških signalov. Overjanje pošiljatelja in prejemnika se tipično neaktivno preverja. Iz dejstva, da lahko napravi ustvarita enake vrednosti na podlagi fizioloških signalov, ki so unikatni za vsako telo,

se predpostavi, da napravi pripadata istemu omrežju. Predpostavlja se, da je nemogoče na telo uporabnika dodati nepooblaščeno senzorsko napravo, ne da bi uporabnik to opazil.

Varovanje, osnovano na podlagi fizioloških signalov, prinaša številne prednosti [128]:

- Uporaba predporazdeljenih skrivnosti ni več potrebna, saj je mogoče te generirati na podlagi zbranih fizioloških signalov.
- Ni potrebe po ločeni fazi vzpostavljanja ključa, saj je mogoče informacije o ključu izmenjati istočasno kot zbrane podatke.
- Izboljša pomnilniško učinkovitost, ker ni treba hraniti trajnih skrivnosti, saj se vsa komunikacija varuje na podlagi meritve signala.
- Omogoča dinamične spremembe v strukturi omrežja, kjer se lahko vozlišča priključujejo v omrežje in izključujejo iz omrežja brez potrebe po spremembah ključev drugih naprav.
- Omogoča priključi in uporabljaj način delovanja, ker lahko vsako vozlišče vzpostavi varno komunikacijo z vsakim drugim vozliščem, ki se nahaja na istem telesu, takoj potem, ko je naprava dodana na telo.

Izzivi vzpostavitve ključa v TSO, ko se to izvaja na osnovi fizioloških podatkov:

- **Energijsko učinkovito delovanje (angl. low-energy design)** [31]: To je posebej pomembna lastnost za vsadke, ki so fizično manjša vozlišča od ostalih in morajo dolgo delovati brez polnjenja, saj niso lahko odstopna.
- **Motnje (angl. interference)**: Ko so si uporabniki TSO dovolj blizu drug drugemu, da so naprave vsakega uporabnika v medsebojnem dosegu, bi naprave na različnih uporabnikih lahko zmotno mislile, da so se v omrežje pridružile nove naprave, in s temi napravami poizkušale vzpostaviti ključ in zatem potencialno z njimi tudi izmenjati podatke [31]. Druge brezžične tehnologije lahko povzročajo motnje v omrežju in preprečijo izmenjavo ključnih informacij [68].
- **Istočasno merjenje fizioloških signalov z visoko entropijo** [31]: Pri uporabi fizioloških signalov za namene vzpostavitve ključa je pomembno, da imajo zajeti podatki visoko entropijo in da so signali, merjeni na dveh ločenih napravah, dovolj podobni, da je iz njih mogoče ločeno zgraditi enaka ključa. Vendar visoka entropija pomeni visoko raven naključnosti v podatkih, kar otežuje zajemanje enakih podatkov na ločenih senzorjih. Da so meritve usklajene in da so zajeti podatki karseda podobni med napravami, je potrebno poskrbeti tudi za istočasni začetek zajemanja podatkov na vsakem senzorju, saj se fiziološki signali skozi čas spreminjajo.
- **Odstranjevanje šuma** [31]: Več neodvisnih senzorjev, ki merijo isti fiziološki signal na različnih delih telesa, zagotovo ne bo zabeležilo identičnih meritev. Zato je pomembno, da obstaja način odstranitve šuma oziroma motenj, ki nastanejo pri različnih merjenjih, tako da je mogoče ujemanje merjenih signalov, čeprav meritve niso nujno popolnoma enake.
- **Prepoznavanje signalov z visoko entropijo** [31]: Raziskovalci se še niso popolnoma uskladili oziroma določili fizioloških signalov, ki imajo dovolj visoko entropijo, da so

primerni za uporabo v protokolih vzpostavitve ključa, čeprav, kot je razvidno iz predlaganih protokolov, je EKG zagotovo najbolj pogosto uporabljen signal.

- **Varnost fizioloških signalov** [31]: Zato da se fiziološki signal lahko uporablja kot vhodni podatek protokolov za vzpostavitev ključa, je ključnega pomena njegova nedostopnost napadalcem. V primeru, da lahko napadalci pridobijo dostop do fiziološkega signala, se varnost komunikacije zruši, saj lahko tudi sami izdelajo vse skrivne ključe, ki se uporabljajo v omrežju.
- **Učinkovito ustvarjanje ključev** [31]: Meritve in obdelava fiziološkega signala, ki se uporabi za vzpostavitev ključa, morajo biti dovolj hitre, da so varovani podatki še vedno relevantni. Pogosto je za to, da lahko dosežemo višjo raven naključnosti zajetih vrednosti, potrebno zajeti večjo količino podatkov, za kar pa je potrebnega več časa.

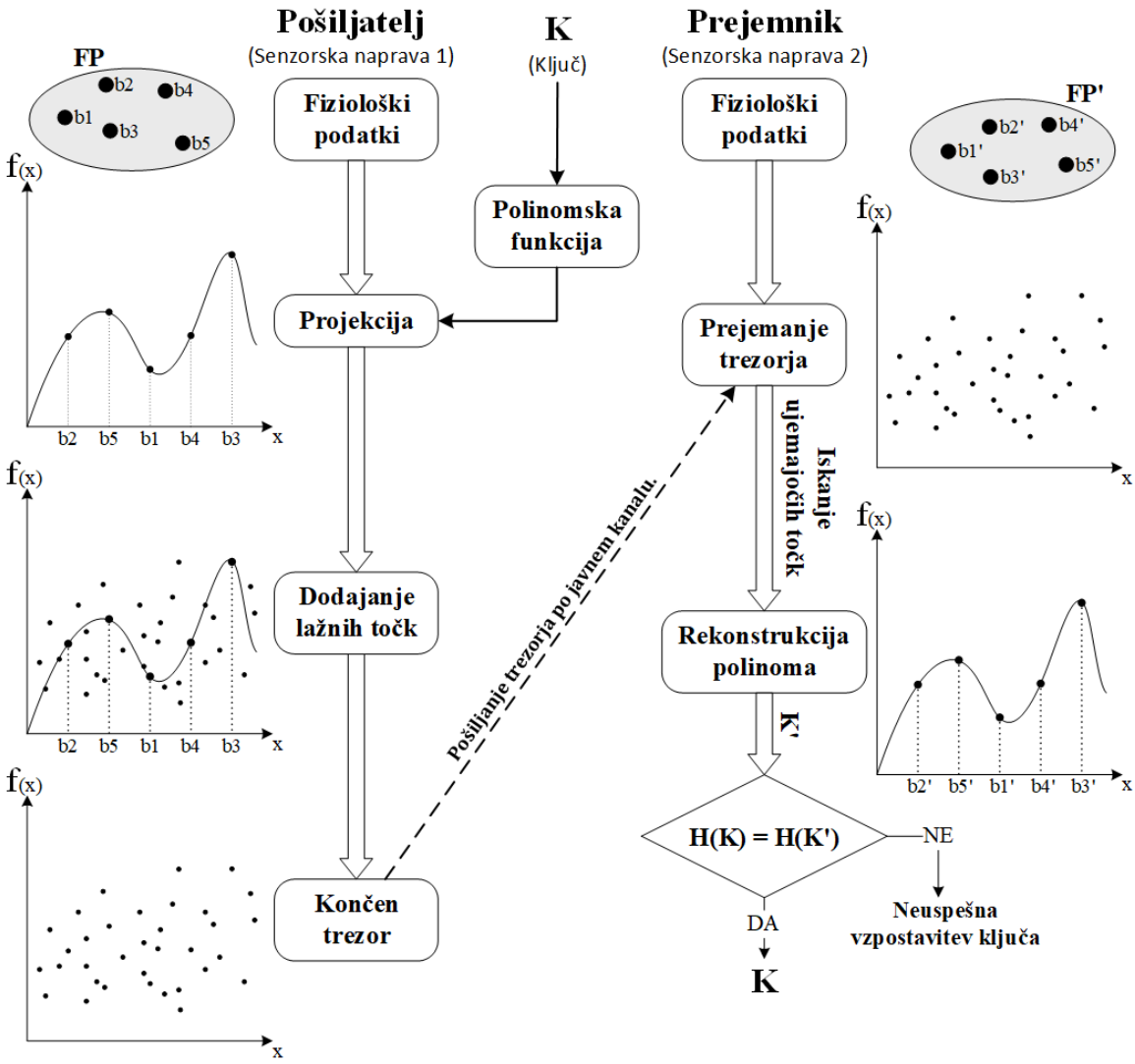
Predhodne raziskave so že predstavile nadaljnje razdelitve protokolov vzpostavitve ključa na osnovi fizioloških ključev. V preglednem članku [31] so bili ločeni glede na vsebovanje predporazdeljenih vrednosti. V novi klasifikaciji smo takšne protokole uvrstili med hibridne, ker vključujejo elemente tradicionalnih in na fizioloških podatkih osnovanih protokolov. Slednji za svoje delovanje ne potrebujejo nobenih predporazdeljenih skrivnosti. V ločeni raziskavi [6] so bili protokoli za vzpostavitev ključa na osnovi fizioloških podatkov razdeljeni v mehko (angl. fuzzy) in nemehko skupino.

Mehke metode, kot sta mehki trezor (angl. fuzzy vault) in mehki prenos (angl. fuzzy commitment), so kriptografski sistemi, ki omogočajo določeno stopnjo odstopanja med "ključem", ki se uporabi za šifriranje, in tistim, ki se uporabi za dešifriranje, ne da bi ta razlika povzročila nezmožnost dešifriranja varovanih vrednosti. Mehke metode so primerne za uporabo pri podatkih, ki pogosto vsebujejo šum, kot so fiziološki podatki. Protokoli z mehkim prenosom preprečujejo vpliv šuma z ločeno skrivno vrednostjo, ki jo uporabijo ob šifriranju podatkov. Čeprav ta vrednost ni ključ, od katerega je odvisna varnost celotnega sistema, je to še vedno skrivna vrednost, ki mora biti znana vsem deležnikom. Ta vrednost je najpogosteje predporazdeljena na naprave. Čeprav takšni protokoli še vedno prinašajo nekaj prednosti, ne izpolnjujejo vseh lastnosti oziroma prednosti, ki smo jih predstavili za protokole vzpostavitve ključa na osnovi fizioloških podatkov. Klasifikacija takšnih protokolov je zelo zahtevna, ker jih tudi avtorji tipično štejejo kot protokole na osnovi fizioloških podatkov, vendar smo jih neglede na to v tej klasifikaciji uvrstili med hibridne, ker vsebujejo predporazdeljene vrednosti.

Posledično se v naši klasifikaciji med mehke protokole uvrščajo predvsem protokoli z mehkim trezorjem, ki pa jih lahko nadalje razdelimo v naslednje skupine [31]: protokoli z mehkim trezorjem (npr. [77, 132, 133, 141–143, 145–148, 151, 152]), protokoli z mehkim trezorjem in kodiranimi lastnostmi (angl. fuzzy vault and encoded features; npr. [129, 135, 153]), protokoli z mehkim trezorjem in kodiranim ključem (angl. fuzzy vault and encoded key materials; npr. [154]) ter protokoli z mehkim trezorjem s kubično krivuljo zlepkov (angl. fuzzy vault with a cubic spline curve; npr. [155]).

Iz števila protokolov, ki uporabljajo mehki trezor, je razvidno, da je to glavna metoda vključitve fizioloških podatkov v protokole vzpostavitve ključa. Mehki trezor je relativno nov

kriptografski konstrukt, prvič predstavljen v [156]. Njegovo delovanje je prikazano na naslednji sliki (Slika 4.1). V protokolih vzpostavitve ključa z mehkim trezorjem pošiljatelj najprej ustvari naključen ključ (K). Njegova vrednost je nato vnesena v polinomsko funkcijo, tako da se ustvarjeni ključ razdeli na manjše kose, kjer se vsak od kosov uporabi kot eden od koeficientov funkcije. Polinomsko funkcijo lahko nadomestimo z drugo funkcijo (npr. kubičnimi zlepki). Zatem potrebujemo vrednosti, s katerimi se "zaklene trezor". Te vrednosti morajo biti poznane vsem deležnikom. V našem primeru so to fiziološki podatki (FP), ki jih naprave pridobijo od telesa, na katerem se nahajajo. Vrednosti fizioloških podatkov, ki so na sliki predstavljene kot x-koordinate (b_1, b_2 …), se ustavijo v zgrajeno polinomsko funkcijo. Rezultati funkcije so y-koordinate točk v grafu. Tem točkam, ki so bile zgrajene na podlagi fizioloških podatkov in ustvarjenega skrivnega ključa, se dodajo lažne točke (angl. chaff points). Te se ustvarijo naključno in jih je veliko več, kot je točk, ki skrivajo informacije o ključu. Njihov namen je zakritje prejšnjih točk. Rezultat je seznam točk, ki ga imenujemo mehki trezor. Ta je skupaj z zgoščeno vrednostjo ustvarjenega ključa ($H(K)$) poslan prejemniku preko javnega kanala. Poleg mehkega trezorja in zgoščene vrednosti bi se lahko posredovali tudi podatki, šifrirani z ustvarjenim ključem. Za odklepanje trezorja mora prejemnik najprej imeti lastne fiziološke podatke (FP'). Te vrednosti (b_1', b_2' …) imajo veliko skupnega s fiziološkimi vednostmi, ki jih je pošiljatelj uporabil (b_1, b_2 …). Prejemnik lahko zato iz grafa z mnogimi točkami izloči točke, ki so bile ustvarjene na podlagi teh vrednosti. Tudi če prejemnik ni pridobil identičnih fizioloških podatkov kot pošiljatelj, bo na podlagi najbližjih točk v grafu lahko z veliko gotovostjo identificiral ustrezne točke. Ta lastnost dovoljuje določeno mero šuma pri zajemanju fizioloških podatkov. Identificirane točke ležijo na polinomski funkciji, ki jo je uporabil pošiljatelj. Na podlagi teh točk lahko prejemnik rekonstruira originalno polinomsko funkcijo. Koeficienti pridobljene funkcije sestavljajo skrivni sejni ključ (K'). Prejemnik preveri pravilnost pridobljenega ključa s pomočjo priložene zgoščene vrednosti ključa, tako da primerja to vrednost z izvlečkom, ki ga ustvari sam z zgostitvijo pridobljenega ključa ($H(K')$).



Slika 4.1: Vzpostavitev ključa s pomočjo mehkega trezorja [132].

Protokoli za vzpostavitev ključa na osnovi fizioloških podatkov, ki ne vsebujejo mehkih trezorjev, so nekoliko bolj redki in med njimi ne prevladuje ena tehnika delovanja. Po zgledu [31] se delijo na: protokole z več prenosi (angl. multiple commitments; npr. [157]), protokole s primerjavo matrik (angl. matrices` comparison; npr. [136, 158]) in protokole z dekodiranjem Reed-Solomon (angl. Reed–Solomon decoding; npr. [159]). Ostali nemehki protokoli vzpostavitve ključa na osnovi fizioloških podatkov, ki smo jih našli v literaturi, so še [60, 128, 131, 137, 139, 144, 160, 161].

Protokol, predstavljen v članku [138], je bil ustvarjen z idejo varovanja osebnih podatkov in omogoča lastniku teh podatkov popoln nadzor nad dostopom do njih. Eden od izzivov v takšnem protokolu je tudi zaznavanje nujnega primera, v katerem uporabnik mogoče ni sposoben dati dovoljena za dostop do svojih zdravstvenih podatkov, ko mora protokol to zaznati in samodejno dovoliti zdravstvenemu osebju dostop. Vzpostavitev ključa v notranjem TSO deluje izključno na podlagi EKG-signalov, medtem ko se za varno vzpostavitev ključa v

zunanjem TSO uporabljajo predporazdeljeni ključi za asimetrično KEK. Vzpostavitev ključa v notranjem TSO deluje tako, da se sejni ključ generira neodvisno na obeh napravah v komunikaciji. Takšno delovanje je značilno za skupino protokolov vzpostavitve ključa z generiranjem skrivnega ključa, ki bo predstavljeno naslednje.

4.3.3 Protokoli vzpostavitve ključa z generiranjem skrivnega ključa

Protokoli vzpostavitve ključa z generiranjem skrivnega ključa omogočajo dvema napravama vzpostavitev simetričnega ključa na podlagi njunega skupnega okolja. V primeru TSO je to skupno okolje uporabnik, na katerem se obe napravi nahajata. Protokoli na osnovi fizioloških podatkov zahtevajo, da vsa senzorska vozlišča v omrežju merijo isti fiziološki signal, na podlagi katerega se izvede vzpostavitev sejnega ključa. To povzroči dodatne strojne zahteve (vozlišča potrebujejo senzor za merjenje signala za meritve, katerim so namenjena, in senzor za merjenje skupnega signala) in omejuje namestitve vozlišč samo na lokacije, kjer je skupni fiziološki signal mogoče meriti (senzorji morajo biti vsaj v stiku s kožo, čeprav mogoče ne merijo fizioloških signalov – npr. pospešek). Ti pogoji za delovanje omejijo uporabnost protokolov za vzpostavitev ključa na osnovi fizioloških podatkov. Protokoli vzpostavitve ključa z generiranjem skrivnega ključa ne omejujejo lokacije, na katere so senzorska vozlišča lahko nameščena, in za svoje delovanje izkoriščajo signale, ki so dostopni vsem napravam.

Protokoli z generiranjem skrivnega ključa in protokoli na osnovi fizioloških podatkov za svoje delovanje uporabljajo signale, ki so specifični za zelo omejeno okolje. V tem sta si obe vrsti protokolov zelo podobni. Najpomembnejša razlika med obema oblikama protokolov je v načinu uporabe merjenih signalov za vzpostavitev ključa. Stanje telesa se ves čas spreminja in fiziološki signali se lahko že sami po sebi nekoliko razlikujejo na različnih delih telesa. Posledično je verjetnost, da bodo meritve takšnih signalov identične na različnih vozliščih, ki se nahajajo na različnih lokacijah, zelo majhna [129]. Zato se v protokolih na osnovi fizioloških podatkov ti podatki uporabljajo za varen transport ključa z ene naprave na drugo. V nasprotju s tem so meritve signalov, ki se uporabljajo v protokolih z generiranjem skrivnega ključa, bolj konsistentne. Zato se te lahko uporabijo na ločenih napravah za neodvisno generiranje sejnega ključa, s katerim se zatem varuje prenos podatkov med napravami, ki so ustvarile ključ. Tako kot protokoli na osnovi fizioloških podatkov imajo protokoli z generiranjem skrivnega ključa zelo dobro razširljivost (uporabljajo signale, do katerih imajo vse naprave dostop, brez potrebe po predporazdeljenih podatkih) in majhno porabo pomnilnika (ni potrebnih trajnih skrivnosti), vendar za svoje delovanje potrebujejo več procesnih operacij.

Med protokoli z generiranjem skrivnega ključa prevladuje uporaba dveh virov signalov. Prvi vir so karakteristike brezžične povezave med napravama, ki želita vzpostaviti ključ. Drugi vir je skupno fizično okolje, v katerem se naprave nahajajo.

Raziskave so pokazale, da je mogoče uporabiti simetrične lastnosti brezžičnega kanala med dvema napravama v komunikaciji za neposredno generiranje skrivnih ključev. Lastnost, ki se za to najpogosteje uporabi, je indikator moči sprejetega signala (angl. received signal strength

indicator – RSSI). Indikator moči sprejetega signala meri moč prejetih radijskih signalov. To metriko lahko merijo vse naprave, ki komunicirajo preko radijskih valov [162]. Prisluškovanje takšnim podatkom nima pomena, saj so karakteristike povezave med prisluškovalcem in izvorom drugačne kot med pošiljateljem in dejanskim naslovnikom. Za zajemanje enakih vrednosti bi torej napadalec moral poustvariti identične okoliščine, kot so v povezavi med pošiljateljem in naslovnikom. To je praktično nemogoče, saj so karakteristike brezžičnih kanalov zelo občutljive na usmeritev in premikanje naprav [163].

Raziskava [164] je pokazala, da je generiranje naključnih vrednosti prepočasno, da bi jih lahko uporabili kot enkratni ščit (angl. one-time pad), ki zagotavlja popolno zaupnost (angl. perfect secrecy). Generiranje naključnih vrednosti je namreč bolj počasno, kot je pridobivanje novih vrednosti, ki bi jih želeli šifrirati. Avtorji so zato ovrgli to idejo in predlagali uporabo istih signalov za izgradnjo simetričnih ključev, ki bi jih lahko menjali na določeno časovno obdobje. Ta ideja je bila dobro sprejeta in danes je generiranje skrivnih ključev uveljavljena metoda, ki je praviloma sestavljena iz štirih korakov [165]. Prvi korak je vzorčenje (angl. sampling phase), v katerem dve ločeni napravi izvedeta meritve signala, na podlagi katerega se generira skrivni ključ. V primeru uporabe karakteristik brezžične povezave med napravama se med napravami pošljejo preiskovalni paketi, na podlagi katerih lahko naprave merijo lastnosti povezave. Naslednji korak je kvantizacija (angl. quantization). Tu se izmerjeni podatki preoblikujejo v ključ. Naslednji korak je faza usklajevanja (angl. reconciliation phase). V tej fazi se razlike, ki so nastale v generiranem ključu med obema napravama kot posledica šuma v kanalu, odstranijo ali popravijo. V zadnjem koraku se ključ, ki je sedaj enak na obeh napravah, okrepi. Ta korak je potreben za preprečevanje koreliranih vrednosti ključa in za preprečevanje potencialnih informacij, ki jih je prisluškovalec lahko pridobil o generiranem ključu v koraku usklajevanja.

Prvi protokol vzpostavitve ključa z generiranjem skrivnega ključa, namenjen uporabi v TSO, ki smo ga našli v literaturi, je [165]. V članku so avtorji pokazali, da je na podlagi meritev karakteristik brezžične povezave med napravama v TSO mogoče ustvariti šifrirne ključe. Potrdili so tudi, da premikanje naprav povzroči nihanja v meritvah indikatorja moči sprejetega signala, kar omogoča hitrejše generiranje ključa. Hitrost generiranja ključa je namreč odvisna od naključnih vrednosti, ki jih lahko naprave pridobijo iz signala. Bolj kot je signal nepredvidljiv (dinamičen), hitreje lahko iz njega pridobivamo naključne vrednosti in posledično je generiranje ključa hitrejše. Avtorji so nadaljevanje raziskave predstavili v članku [166], v katerem so potrdili ugotovitve, predstavljene v prvem članku, in preverili uporabnost protokolov vzpostavitve ključa z generiranjem ključa na vozliščih, ki so nameščena na različnih delih telesa, kjer bi lahko prišlo do težav zaradi nesorazmernega premikanja naprav (naprave na trupu, rokah in nogah). V istem članku so predstavili tudi rešitve za izboljšanje ujemanja meritev med napravami. V tretjem članku [163] izpostavijo časovno razliko v zajemanju podatkov kot glavni vzrok za neskladje meritev med napravami in predlagajo zajemanje podatkov za namene generiranja ključa samo v obdobjih aktivnosti telesa, kar zmanjša verjetnost neskladja med meritvami vozlišč.

Za prvim predlaganim protokolom vzpostavitve ključa z generiranjem skrivnega ključa v TSO je bilo predstavljenih še veliko drugih protokolov, ki uporabljajo indikator moči sprejetega

signala kot vhodne podatke za generiranje simetričnega sejnega ključa [74, 167–176]. Skoraj vsak od teh člankov uvede tudi izboljšavo delovanja.

Članek [167] predlaga uporabo že obstoječih paketov, ki se pretakajo med napravama, za meritve indikatorja moči sprejetega signala, namesto namenskih preiskovalnih paketov in na takšen zmanjšati količino poslanih in prejetih podatkov. Predlagajo tudi uporabo razlike med zaporedoma izmerjenimi indikatorji moči sprejetega signala. Potem ko je bilo zbranih dovolj takšnih razlik, lahko naprave enostavno s povprečno vrednostjo ugotovijo dinamičnost zajetih signalov. V primeru visoke povprečne vrednosti je bilo veliko sprememb v meritvah. Kot smo prej omenjali, so takšne meritve veliko bolj primerne za ustvarjanje naključnega ključa. Če variabilnost zajetih podatkov ni dovolj visoka, se zajete meritve zavržejo. Tak postopek se ponavlja, dokler naprave ne zberejo dovolj naključnih vrednosti za celoten ključ.

V takšnih protokolih vzpostavitve ključa je overjanje pogosto izpuščeno in se šteje kot ločena funkcionalnost, ki mora biti naknadno zagotovljena. Protokol [74] je bil naknadno nadgrajen v članku [170], v katerem so avtorji uporabili iste vrednosti indikatorja moči sprejetega signala za generiranje skrivnega ključa in overjanje naprav.

Ideja o uporabi naprav z dvema antenama je bila predstavljena v [172]. Z uporabo vsaj ene naprave (tipično je to bazna postaja), ki ima dve ločeni anteni, je mogoče oddajanje in prejemanje paketov opraviti na naključni od obeh anten. Meritve karakteristik kanala se zato spreminjajo med meritvami in to omogoča večjo raznolikost med zajetimi podatki. Takšno delovanje dodatno oteži prisluškovanje in izboljša hitrost generiranja novih ključev, predvsem v situacijah, ko se uporabnik ne premika. Ta izboljšava je zelo pomembna, predvsem za uporabnike, ki se ne morejo veliko premikati (npr. bolniki v bolniški postelji). Predlagani protokol vsebuje tudi overjanje naprav, medtem ko tega protokola, predstavljena v [173, 174], ki sta tudi bila ustvarjena za delovanje na napravah z dvema antenama, ne omogočata. Avtorji [173] se osredotočijo na hitrost generiranja ključev, ki jo ponovno izboljšajo v primerjavi s predhodnim protokolom, kot tudi zmanjšajo korelacijo med zaporednimi meritvami, medtem ko [174] uporabi frekvenčno skakanje (angl. frequency hopping). Protokol, predstavljen v treh člankih [162, 175, 177], uporabi dinamično frekvenčno skakanje in dve anteni na eni napravi za ustvarjanje umetne naključnosti na kanalu, kar omogoča hitro generiranje ključev, ki ni odvisno od premikanja naprav.

Vsi opisani protokoli, ki delujejo na podlagi meritev indikatorja moči sprejetega signala, so namenjeni samo uporabi med napravami, ki so neposredno povezane – so v dometu signala. Protokol, predstavljen v [176], omogoča generiranje ključa na vozliščih, ki komunicirajo posredno. Za to je potrebno zaupanja vredno vmesno vozlišče, ki sodeluje pri vzpostavitvi ključa.

Protokol, predstavljen v [168], je edini protokol, ki smo ga našli v literaturi in uporablja meritve indikatorja moči sprejetega signala za namene varovanja transporta ključa namesto generiranja ključa. Za svoje delovanje uporablja mehki trezor. Postopek ustvarjanja in odklepanja trezorja je enak, kot smo ga predstavili v protokolih vzpostavitve ključa na osnovi

fizioloških podatkov, le da se namesto fizioloških signalov uporabi indikator moči sprejetega signala.

Druga skupina protokolov za vzpostavitev ključa z generiranjem skrivnega ključa generira ključe na podlagi skupnega fizičnega okolja naprav, ki vzpostavljajo ključ. Protokoli delujejo na ideji okolijskih pogojev, ki si jih naprave delijo. Naprave merijo te pogoje in na podlagi teh meritev neodvisno ustvarijo skrivni ključ ali pa s pomočjo teh meritev izmenjajo ključ. Merjeni okolijski pogoji morajo biti specifični za vsakega uporabnika, tako da meritve vežejo napravo na posameznega uporabnika. To je pomembna lastnost merjenih signalov, ki omogoča overjanje naprav in otežuje njihovo ponarejanje [178]. Če ti signali niso specifični za vsakega uporabnika, generirani ključi niso skrivni, saj jih lahko ustvarijo tudi naprave, ki niso del istega TSO. Uporaba signalov skupnega fizičnega okolja za namene vzpostavitve ključa z generiranjem skrivnega ključa je enaka, kot je bila pri uporabi karakteristik brezžičnih povezav. Proces merjenja in preoblikovanja zajetih vrednosti v sejni ključ sledi istim štirim korakom, kot so bili predstavljeni pri protokolih na osnovi karakteristik brezžičnih povezav: vzorčenje, kvantizacija, usklajevanje in ojačenje ustvarjenega ključa.

Raziskave takšnega delovanja se v TSO osredotočajo na merjenje pospeškov, ki jih imajo naprave na telesu. Takšni signali izpolnjujejo prejšnje pogoje, saj lahko samo naprave, ki so nameščene na telo, merijo pospeške tega telesa. Dobra lastnost protokolov z generiranjem skrivnega ključa na podlagi karakteristik brezžičnega kanala je to, da ne zahtevajo dodatne strojne opreme na senzorskih vozliščih za njihovo delovanje. Po drugi strani protokoli, ki delujejo na podlagi merjenja pospeškov, zahtevajo uporabo naprav z merilnikom pospeška (angl. accelerometer). Posledično so takšna vozlišča bolj kompleksna in dražja. Druga pomanjkljivost uporabe pospeška v primerjavi s karakteristikami brezžične povezave je njihovo nedelovanje na telesih, ki niso v gibanju. Čeprav so protokoli vzpostavitve ključa z generiranjem skrivnega ključa na podlagi karakteristik povezave tudi imeli te težave, so jih naprednejši protokoli rešili z uporabo večjega števila anten in frekvenčnega skakanja. To v protokolih, ki delujejo na podlagi merjenja pospeškov, ni mogoče. Zato je generiranje ključev v takšnih protokolih na negibnih uporabnikih zelo počasno in neučinkovito. Lokacija naprav na telesu lahko tudi predstavlja velik izziv za protokole, ki delujejo na podlagi merjenja pospeškov. Težave lahko povzročajo predvsem prostorska poravnava vseh treh osi med napravami in razlike v pospeških, ki so prisotni na različnih delih telesa (npr. zaradi zibanja rok pri hoji bodo pospeški naprav, ki so nameščene na zapestje, različni od meritev naprav, ki so na trupu uporabnika).

Prvi protokoli vzpostavitve ključa z generiranjem skrivnega ključa, ki so delovali na osnovi podatkov o pospešku naprave, so imeli veliko omejitev, povezanih s predstavljenimi problemi. Naprave, ki so delovale z enim od prvih takšnih protokolov [179], so generirale ključ, tako da jih je uporabnik vzel v roko in istočasno stresel, dokler niso neodvisno ustvarile vsaka svojega identičnega ključa. Na takšen način so bile naprave podvržene enakim pospeškom in njihova usmeritev se ni spreminjala med tresenjem. Protokol [180] je prav tako zahteval, da je uporabnik vzel v roko naprave in jih namenoma stresal, dokler niso vzpostavile ključa, s tem da je novejši protokol vseboval tudi overjanje naprav. Protokoli s takšnim delovanjem, kjer

mora uporabnik namenoma stresati naprave v roki, so omejeni in se lahko uporabljajo samo na napravah, ki jih lahko uporabnik odstrani s telesa. Takšno delovanje tudi izključuje možnost samodejnega spreminjanja ključa, saj vedno vključuje sodelovanje uporabnika.

Merjenje pospeška na različnih delih telesa je težava, ker so izmerjene vrednosti seštevek premikanja različnih delov telesa. Vse naprave merijo pospeške hoje, ki je specifična za vsakega uporabnika. Naprave, nameščene na telo, merijo pospeške hoje, medtem ko naprave, nameščene na okončine, merijo tudi pospeške premikanja nog oziroma zibanja rok. Zato da lahko te naprave generirajo enak ključ, je potrebno na primer za naprave, ki so nameščene na rokah, odstraniti pospešek zibanja rok od zajetih meritev, zato da bodo vrednosti predstavljale le pospeške hoje in bodo primerljive z meritvami, zajetimi na vozličih, ki so na trupu uporabnika. Raziskovalci so naslovili to problematiko v članku [181] in predstavili protokol, ki omogoča delovanje na napravah, ki so prosto nameščene kjer koli na telesu. Avtorji so predlagali tudi rešitev za težavo usklajevanja začetka meritev signalov, na podlagi katerih se izvede vzpostavitev ključa. Ta težava je prisotna povsod, kjer so potrebne enake meritve na ločenih napravah. Kot rešitev pri uporabi pospeška so predlagali dogovor med vozlišči, da začnejo beležiti pospešek in generirati ključ, potem ko zaznajo udarec pete pri hoji. Problematiko prostorske poravnave pa rešijo, tako da vrednosti vseh treh osi združijo v skupno vrednost, ki ni odvisna od orientacije naprav. V članku [182] so isti avtorji nadgradili prvi protokol s spremenjeno metodo kvantizacije, ki je omogočala hitrejše generiranje naključnih vrednosti skrivnega ključa, vendar ob nekoliko slabši usklajenosti med napravami (te neskladnosti so naknadno odstranili).

Protokoli, ki delujejo na podlagi skupnega fizičnega okolja naprav, lahko ravno tako uporabijo zbrane podatke za zaščiten transport ključa, kar je bolj tipična oblika delovanja protokolov vzpostavitve ključa na osnovi fizioloških podatkov. Protokol, predstavljen v [183], uporabi signale pospeška za ustvarjanje naključnega ključa. Zatem te iste podatke s kvantizacijsko metodo, predstavljeno v [173], pretvori v podatke, s katerimi zaklene prej ustvarjeni ključ v mehki trezor, ki ga posreduje naslovniku. Prejemnik lahko odklene mehki trezor, ker ima dostop do enakih meritev pospeška.

Protokoli v tej skupini lahko uporabljajo tudi druge signale iz skupnega okolja, kot so podatki o pospešku. Članek [184] opisuje protokol za vzpostavitev ključa z generiranjem skrivnega ključa na podlagi avdio signalov okolice. V članku [185] je protokol prilagojen za uporabo s signali pospeška.

4.3.4 Hibridni protokoli vzpostavitve ključa

Hibridni protokoli vzpostavitve ključa so mešanica dveh drugih vrst protokolov. V veliki večini hibridni protokoli združujejo uporabo fizioloških podatkov s predporazdeljenim skrivnim materialom, z namenom ustvariti boljši protokol vzpostavitve ključa, kot ga je mogoče doseči z uporabo posamezne metode. Pri razvoju protokolov za vzpostavitev ključa na osnovi fizioloških podatkov se predpostavlja, da napadalec ne bo imel možnosti pridobitve fizioloških

signalov. Zato da bi lahko to dosegel, bi napadalec moral na žrtev namestiti lastno napravo, ki bi merila fiziološke signale, ki se uporabljajo za vzpostavitev ključa. Storiti kaj takega, ne da bi uporabnik to opazil, je skoraj nemogoče. Dejstvo, da se v protokolih uporabljajo trenutni podatki, dodatno zmanjša verjetnost pridobitve teh podatkov in praktično izniči verjetnost dolgotrajnega vpogleda napadalca v dani fiziološki signal, saj bi za to morale biti napadalčeve naprave vedno prisotne na telesu. Kljub temu je mogoče, da bi napadalec pridobil potrebne fiziološke podatke za omejen čas. Zato se protokoli na osnovi fizioloških podatkov združujejo s predporazdeljenim ključem, ki varuje proces vzpostavitve ključa, tudi če je bil fiziološki signal razkrit. Združevanje različnih pristopov ima lahko različne pozitivne vplive na delovanje protokola.

V poglavju o protokolih vzpostavitve ključa na osnovi fizioloških signalov so že bili omenjeni protokoli, ki delujejo s pomočjo mehkega prenosa. Ti protokoli za svoje delovanje potrebujejo vrednost za odpravljanje napak (angl. error correction code), ki je tipično predporazdeljena na naprave v omrežju. Zato se uvrščajo med hibridne protokole, čeprav so pogosto predstavljeni kot protokoli na osnovi fizioloških podatkov. Primerov takšnih protokolov je kar nekaj [17, 69, 130, 186]. V članku [31] razdelijo protokole, ki vsebujejo uporabo fizioloških signalov in predporazdeljenih skrivnosti, na: protokole s fiziološkim certifikatom (angl. physiological certificate; npr. [187]), protokole z večtočkovnim pogajanjem o ključu (angl. multipoint key negotiation; npr. [140]) in protokole na osnovi fizioloških podatkov s predporazdeljenimi ključi (npr. [188]).

Poleg tega obstaja še veliko drugih načinov, ki so jih različni avtorji uporabili za združevanje preddistribucije skrivnega materiala in fizioloških podatkov. V članku [189] je predstavljen hibridni protokol, ki deluje na enak način kot Diffie-Hellmanov protokol, le da naključne vrednosti generira na podlagi zajetih fizioloških podatkov. Podoben pristop je uporabljen tudi v protokolih za vzpostavitev ključa, predstavljenih v člankih [71, 190, 191], ter nadgradnji tega protokola [192], ki v osnovi delujejo enako kot tradicionalni protokol s predporazdeljenimi ključi. Kar jih razlikuje od tradicionalnih protokolov, je uporaba fizioloških podatkov, ki jih senzorska vozlišča v omrežju merijo, za izgradnjo novih sejnih ključev.

Protokol, predstavljen v [134], je zelo preprosta kombinacija uporabe obeh metod varne vzpostavitve ključa v TSO. Fiziološki podatki s tehniko interpolacije kubičnih zlepkov varujejo naključno ustvarjen ključ. Nastala vrednost je dodatno zaščitena, tako da je šifrirana s predporazdeljenim ključem. Kombinacija obeh pristopov varuje v primeru, da je odtujen trajni (predporazdeljen ključ), ali v primeru, da napadalec pridobi dostop do trenutnih fizioloških podatkov. Vzpostavitev ključa je še vedno ranljiva, če napadalec pridobi obe vrednosti (trajni ključ in fiziološke podatke). Podoben pristop je uporabljen tudi v protokolu, predstavljenem v člankih [193, 194]. Raziskava [195] predstavi še en podoben protokol, le da ta za varovanje sejnega ključa, ustvarjenega s pomočjo fizioloških podatkov, uporablja KEK in avtorji predvidijo uporabo fizioloških podatkov, ki bodo dolgotrajno prepoznavni, tako kot je na primer prstni odtis.

Protokol, predstavljen v [196], deluje kot protokol na osnovi fizioloških vrednosti s predporazdeljenim ključem, ki je namenjen varovanju komunikacije v primeru, da je bazna postaja kompromitirana. Avtorji protokola [197] uporabijo fiziološke podatke za posodabljanje sejnega ključa. To storijo tako, da obstoječi ključ združijo z zgoščeno vrednostjo izmerjenih fizioloških podatkov.

Avtorji raziskave [198] so predlagali uporabo biometričnega šifriranja. V protokolu pošiljatelj najprej zbere fiziološke podatke in jih priredi z valčno transformacijo (angl. wavelet transform) ter v zgoščevalni funkciji združi z vrednostjo, predporazdeljeno na naprave v omrežju. Nad rezultatom zgoščevanja se izvede koda Reed-Solomon, ki omogoča odpravo neskladij, ki lahko nastanejo pri merjenju fizioloških podatkov na ločenih vozliščih in povzročijo neskladje zajetih vrednosti. Med ustvarjeno vrednostjo in ločeno ustvarjenim naključnim sejnim ključem se opravi operacija XOR. Nastala vrednost je varna za prenos v omrežju in iz nje lahko prejemnik na podlagi merjenja istih fizioloških signalov in predporazdeljene vrednosti izlušči posredovan sejni ključ.

Protokol, predstavljen v [199], je v svojem namenu in delovanju zelo podoben protokolu iz [138]. Omogoča vzpostavitev varne komunikacije med vgrajenimi telesnimi senzorji in zdravstvenimi centri preko osebnega strežnika, ki igra ključno vlogo pri overjanju entitet in vzpostavitvi ključa. Kljub podobnostim med obema protokoloma uporablja ta predporazdeljene asimetrične ključe na senzorskih vozliščih, zaradi česar ga uvrščamo med hibridne protokole.

5 Vrednotenje varnosti in učinkovitosti protokolov za vzpostavitev ključa v telesnih senzorskih omrežjih

Po pregledu člankov, ki predstavljajo nove protokole za vzpostavitev ključa, namenjene za uporabo v TSO, in njihovi razvrstitvi v štiri glavne skupine protokolov je bila izvedena analiza metod, ki jih avtorji uporabljajo za namene preverjanja ustreznih varnostnih lastnosti ter učinkovitosti predlaganih protokolov. Na podlagi zbranih informacij o najpogostejših metodah, ki se uporabljajo v znanstveni literaturi, bomo izbrali metode, ki jih bomo kasneje uporabili pri analizi varnosti in učinkovitosti novih protokolov, razvitih v disertaciji.

5.1 Metode vrednotenja varnosti protokolov

V tem delu disertacije bomo pregledali in analizirali različne metode, ki jih raziskovalci uporabljajo za preverjanje varnostnih lastnosti in odpornosti na napade predlaganih protokolov vzpostavitve ključa, namenjenih uporabi v TSO.

5.1.1 Hevristično vrednotenje varnosti

Po pregledu vseh protokolov za vzpostavitev ključa, ki so bili predlagani za uporabo v TSO, je postalo jasno, da je najbolj pogosta metoda, ki so se je avtorji posluževali za vrednotenje oziroma dokazovanje varnosti predlaganih protokolov, neformalna opisna oblika – hevristična (angl. ad hoc) metoda vrednotenja. To pomeni, da ne obstaja standardizirano zaporedje korakov, ki pokaže varnostno raven analiziranega protokola. Avtorji sami ustvarijo scenarije napada, predstavijo, kako predlagani protokoli varujejo pred takšnimi okoliščinami, in opišejo, kako in zakaj specifično delovanje protokola izpolnjuje posamezne varnostne lastnosti. V spodnji tabeli (Tabela 5.1) se nahaja seznam vseh protokolov vzpostavitve ključa, namenjenih delovanju v TSO, ki smo jih našli med pregledom literature in ki vsebujejo hevristično preverjanje varnosti. Protokoli so v tabeli predstavljeni kot reference na članke, v katerih so predstavljeni ali opisani. Drugi stolpec v tabeli prikaže razvrstitev danega protokola glede na predstavljen klasifikacijski model (T = tradicionalni protokol, F = protokola na osnovi fizioloških podatkov, G = protokol z generiranjem skrivnega ključa in H = hibridni protokol). Na podlagi varnostnih zahtev in napadov na takšne protokole (glej poglavji 4.1 in 4.2) smo v tabelo uvrstili najpomembnejše in v analizah najpogosteje omenjene lastnosti in napade. Celica na preseku posameznega protokola in varnostne lastnosti je označena z "X", če je ta lastnost oziroma odpornost na napad bila opredeljena v analizi članka. Prazna polja ne pomenijo samodejno, da določen protokol ne zagotavlja obrambe pred dano ranljivostjo, ampak zgolj, da

odpornost na takšen napad oziroma ta varnostna lastnost ni bila omenjena v analizi. Določeni napadi so mogoči samo v zelo specifičnih okoliščinah, zato pogosto niso omenjeni v analizah protokolov, ker takšni napadi v teh protokolih niso mogoči. Kot smo omenili, v tabeli niso zbrani vsi možni napadi, temveč samo tisti, ki so dovolj pogosti, da smo jih zasledili v več člankih različnih avtorjev.

Tabela 5.1: Seznam protokolov vzpostavitve ključa v TSO in njihove varnostne lastnosti.

Protokol	Klasifikacija	Zaupnost podatkov	Overjanje vozlišč	Celovitost podatkov	Napad z ujemanjem	Napad s ponavljanjem ali svežina	MITM ali obojestransko overjanje	Napad ugibanja gesla	Napad sledenja ali nepovezljivost	Prihodnja varnost/pretekla varnost	Razširljivost	Napad za zavrnitev storitve	Kompromitirano vozlišče	Neponaredljivost	Napad pooseblјanja	Napad zarote	Napad s klonom
[19]	T	X			X	X	X	X						X			
[20]	T					X	X	X						X	X		
[96]	T	X	X	X		X							X		X		
[117]	T		X							X			X			X	X
[120]	T										X						
[121]	T									X						X	
[125]	T															X	
[127]	T	X		X		X			X	X/		X					
[115]	T							X						X	X		
[116]	T						X			X/						X	
[85]	T					X	X					X					
[97]	T	X	X	X						X	X		X				
[98]	T	X	X	X													
[95]	T	X		X		X											
[84]	T	X	X	X	X				X				X				
[80]	T	X	X	X						X	X		X				
[103]	T					X							X				
[86, 113]	T	X			X								X				
[104]	T		X				X			X/					X		
[109]	T	X				X	X		X								
[122]	T	X	X	X		X					X	X					

[105, 106]	T		X				X			X/							
[107]	T	X	X	X						X	X						
[87]	T					X	X	X						X			X
[75]	T					X	X			X/				X			
[123]	T	X	X	X		X	X	X	X	X			X		X		
[90]	T					X	X		X	X			X	X	X		
[60]	F					X	X										
[139]	F					X					X	X					
[77]	F	X	X	X		X	X	X	X								
[145]	F	X	X	X													
[146]	F					X	X										
[135]	F	X	X	X		X	X										
[137]	F	X	X	X		X											
[128]	F	X	X	X		X											
[196]	H	X	X	X		X							X	X			
[71]	H	X	X	X													
[134]	H	X		X		X	X		X								
[188]	H	X	X	X		X	X										
[192]	H	X	X			X				X/		X	X				
[193]	H	X		X		X											
[194]	H	X	X	X		X											
[195]	H	X	X	X		X											
[199]	H						X										
[198]	H	X	X	X		X	X	X	X	X							
[74, 170]	G		X				X								X		

X – Analiza varnosti protokola omenja ta napad oz. lastnost in protokol je vsaj delno odporen na napad oz. izpolnjuje to lastnost.

Prazna celica – Članek ne vsebuje analize določene ranljivosti protokola oz. varnostne lastnosti ali protokol ni odporen na dani napad oz. ne izpolnjuje varnostne lastnosti.

T, F, H in G – Tipi protokolov za vzpostavitev ključa v TSO glede na predlagano klasifikacijo.

X/ – Protokol izpolnjuje pogoje prihodnje varnosti, vendar ne izpolnjuje pogojev pretekle varnosti oz. ta ni omenjena v članku.

V tabeli (Tabela 5.1) manjkajo: napad odseva (angl. reflection attack) [60], napad posrednika [60], namerno motenje (angl. Jamming) oziroma napad korupcije povezave (angl. link corruption attack) [114, 123], razkritje kratkotrajnega ključa (angl. ephemeral secret key leakage attack ali known-key security) [20, 123], ugibanje skrivnosti privzetega prehoda (angl. gateway secret guessing attack) [19], napad poosebljanja s kompromitiranim ključem [105, 106], poplavljanje s hello sporočili [128, 187, 192] ter drugi usmerjevalni napadi (napad

požiralnika, napad selektivnega posredovanja [139], napad Sybil in napad s črvino), ki so bili upoštevani v člankih [122, 128, 160]. Poleg teh napadov je v člankih omenjena tudi lastnost ključev, ki omogoča, da se ključ večkrat prekliče [134, 198]. Ta lastnost se omenja izključno v protokolih, ki vsebujejo uporabo fizioloških signalov in imajo specifično delovanje, zato te lastnosti nismo vključili v tabelo. V tabelo prav tako ni vključen napad prisluškovanja, saj se odpornost na takšne napade šteje kot minimalna raven zagotavljanja varnosti, ki bi jo moral doseči vsak protokol.

Iz števila posameznih tipov protokolov v tabeli je razvidno, da je hevristična metoda preverjanja varnosti zelo pogosto uporabljena v tradicionalnih protokolih, medtem ko avtorji protokolov vzpostavitve ključa na osnovi fizioloških podatkov in protokolov z generiranjem skrivnega ključa redkeje uporabijo to metodo. Izjema temu je napad vrnjenega napadalca, ki je ena najhujših in najbolje poznanih oblik napadov. Posledično je varovanje pred takšnim napadom pogosto opredeljeno tudi v protokolih vzpostavitve ključa na osnovi fizioloških podatkov in protokolih z generiranjem skrivnega ključa [129, 168, 181, 182].

5.1.2 Formalno preverjanje varnosti

Za preverjanje varnosti obstajajo tudi formalni modeli, s katerimi je mogoče preveriti varno delovanje protokola. Formalni model v celoti in nedvoumno opisuje delovanje protokola z dobro določeno sintakso in semantiko, tako da omogoča sistematično analizo protokola na podlagi logičnih pravil. BAN-logika (angl. BAN logic) je model, namenjen formalnemu preverjanju protokolov overjanja in vzpostavitve ključa [19]. Predstavljena je bila v [200] in je poimenovana po njenih iznajditeljih – Burrows, Abadi in Needham. BAN-logika omogoča izdelavo dokaza o pravilnem delovanju protokola, vendar je pravilno delovanje modela odvisno od predpostavk. Zato tudi formalni dokaz z BAN-logiko ne zagotavlja popolne garancije delovanja protokola brez možnih varnostnih pomanjkljivosti. Strogo določena oblika takšnih dokazov predpostavlja idealne okoliščine delovanja, ki pa so zelo redke v realnem svetu. BAN-logika ima lastno sintakso za izraze, izjave, ki jih je mogoče izdelati, in pravila, ki se ustvarijo z združevanjem izrazov in izjav. Primerna je za uporabo predvsem v tradicionalnih protokolih [117]. To potrjuje tudi seznam člankov, kjer je bila BAN-logika uporabljena za varnostno analizo protokolov, ki so vsi tradicionalne oblike [19, 20, 75, 90, 109, 123]. Čeprav BAN-logika zagotavlja formalni model preverjanja protokolov, je njena uporaba zelo redka, vendar postaja pogostejša v novejših protokolih. Še redkeje uporabljena je SVO-logika [201], ki je nastala kot združitev predhodnih modelov, vključno z BAN-logiko. Uporabo SVO-logike smo zasledili samo v enem članku [198].

5.1.3 Delno formalno preverjanje varnosti

Med delno formalno preverjanje varnosti protokolov uvrščamo različna orodja, ki so namenjena samodejnemu preverjanju varnostnih lastnosti oziroma pomanjkljivosti varnostnih protokolov. AVISPA (angl. Automated Validation of Internet Security Protocols and

Applications) [202] je orodje za samodejno preverjanje internetnih varnostnih protokolov in aplikacij. Zagotavlja modularni in izrazni formalni jezik za definiranje protokolov in njihovih lastnosti. Omogoča širok nabor tehnik samodejne analize, s katerimi se preizkusi definiran protokol. AVISPA ima grafični vmesnik, ki uporabniku omogoča, da definira svojo shemo in izbere testne metode in njene parametre. Med pregledom literature smo ugotovili, da je tako kot BAN-logika tudi orodje AVISPA redko uporabljeno za preverjanje varnosti protokolov vzpostavitve ključa namenjenih uporabi v TSO. Od skupno 116 člankov samo štirje vsebujejo analizo z orodjem AVISPA [90, 122, 134, 135]. Poleg orodja AVISPA obstaja še nekaj drugih – ProVerif, Scyther, Tamarin Prover in Alloy analyzer – vendar uporabe teh orodij nismo zasledili v analizah protokolov vzpostavitve ključa, namenjenih uporabi v TSO.

5.1.4 Preverjanje varnosti v protokolih na osnovi fizioloških podatkov

Tako kot se protokoli vzpostavitve ključa na osnovi fizioloških signalov razlikujejo od tradicionalnih protokolov vzpostavitve ključa, se tudi metode preverjanja varnostnih lastnosti in odpornosti na napade med oblikami protokolov razlikujejo. Kot smo pokazali v prejšnjih treh podpoglavjih, protokoli vzpostavitve ključa na osnovi fizioloških podatkov zelo redko uporabijo hevristično, formalno ali delno formalno metodo preverjanja varnosti protokola. Analiza varnosti v primeru takšnih protokolov se osredotoča predvsem na varnostne lastnosti uporabljenih fizioloških signalov in mehkih mehanizmov, ki se uporabljajo v veliki večini protokolov na osnovi fizioloških podatkov. Uporaba fizioloških signalov nosi s seboj tveganje kompromitiranja signala ali oddaljenega zajemanja fiziološkega signala [128]. Oddaljeno zajemanje EKG-signala s pomočjo kamer je omenjeno v [199]. Za uporabo fiziološkega signala je pomembno, da so vrednosti, ki nastanejo na podlagi signala, naključne. Raziskovalci v člankih [15, 138, 199] s statističnimi testi pokažejo, da so vrednosti, ki jih pridobivajo v protokolih, statistično naključne.

Velik delež varnostnih analiz je usmerjen v varnost mehkih trezorjev. Razlogi so predvsem njihova pogosta uporaba in pa dejstvo, da je mehanizem relativno nov in še nepreizkušen. Varen prenos sejnega ključa pri vzpostavitvi ključa v protokolih z mehkim trezorjem je odvisen od trezorja, ki vsebuje zakrit sejni ključ in je posredovan med napravami preko javnega kanala. Preneseni trezor lahko zato napadalec preprosto prestreže in poizkuša iz njega pridobiti varovano vrednost. Varnost trezorja je odvisna primarno od števila lažnih točk v trezorju in od stopnje uporabljene polinomske funkcije. Obe lastnosti sta bili raziskani v [129, 132, 147], medtem ko so raziskave v [133, 146, 159] potrdile, da je najpomembnejša lastnost za varovanje trezorja število lažnih točk. Članek [151] je tudi primerjal, kakšne učinke ima spreminjanje števila lažnih toč v različnih protokolih. Poleg stopnje polinomske funkcije in števila lažnih točk so avtorji [154] pokazali, da so za varnost mehkih trezorjev pomembne tudi vrednosti, ki se pridobijo iz fizioloških signalov, in izbira lažnih točk. Poleg tega so avtorji v [155] še raziskali vpliv velikosti sejnega ključa na varnost trezorja, medtem ko so avtorji [151] podali formalen dokaz o odpornosti mehkih trezorjev na napade z izbranim čistopisom (angl. chosen plaintext attack).

5.1.5 Preverjanje varnosti v protokolih z generiranjem skrivnega ključa

Najpogostejša metrika ocenjevanja varnosti protokolov vzpostavitve ključa z generiranjem skrivnega ključa v TSO je ocena entropije, ki je prisotna v generiranih nizih. Entropija je mera negotovosti oziroma naključnosti v nizu bitov, ki je v primeru protokolov z generiranjem skrivnega ključa ustvarjen iz okoliškega signala, ki ga protokol uporablja. Višja entropija pomeni več naključnosti v generiranem nizu bitov in posledično manjšo odvisnost med posameznimi biti v nizu. Praktično vsi avtorji za namene ocene entropije uporabljajo NIST-ovo zbirko testov (angl. Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications) [203]. Članki [162–164, 167, 168, 172–177, 179–182] vključujejo oceno entropije generiranih vrednosti.

Protokoli, ki uporabljajo karakteristike brezžične povezave, pogosto vključujejo analizo odpornosti na napade tvorjenja žarkov (angl. beam-forming attacks) [74, 170, 172], medtem ko morajo protokoli z generiranjem skrivnega ključa na podlagi signalov pospeška upoštevati možnost napada poosebljanja, kjer želi napadalec posnemati hojo žrtve [181, 182]. Protokoli z mehkim trezorjem se tako kot protokoli na osnovi fizioloških podatkov za višanje ravni varnosti zanašajo predvsem na število lažnih točk [168, 183].

5.1.6 Ostale metode preverjanja varnosti

Nekatere analize predstavljenih protokolov so skrajno omejene ali vsebujejo elemente, ki niso tipično uporabljeni v analizah in so specifični posameznim člankom. Ne glede na kakovost analize ali njeno edinstvenost vključujejo tudi članki [99, 110, 118–120, 136, 157, 158, 171, 186–190, 204] analize varnosti predstavljenih protokolov.

5.2 Razprava o vrednotenju varnosti protokolov za vzpostavitev ključa v TSO

Večina raziskav, ki predstavljajo nov protokol za vzpostavitev ključa v TSO, vključuje tudi analizo varnostnih lastnosti novega protokola. Kot je razvidno iz pregleda metod, ki jih avtorji uporabljajo, je najpogostejši pristop neformalno oziroma hevristično preverjanje protokola. To pomeni, da za namene merjenja oziroma dokazovanja varnosti in odpornosti protokola na napade niso uporabljeni standardizirani postopki. Avtorji ustvarjajo scenarije za predstavitev varnosti sheme ali pa samo opisujejo posamezne dele protokola in kako ti zagotavljajo varnost. Vrednotenje varnosti s formalnimi in delno formalnimi metodami je zelo redko, vendar smo zaznali, da se frekvenca uporabe izboljšuje v novejših protokolih.

Pri zbiranju podatkov o hevrističnem vrednotenju, ki smo jih strnili v tabeli (Tabela 5.1), smo zasledili, da avtorji pogosto v svojih raziskavah omenjajo samo najpreprostejše varnostne lastnosti in oblike napadov ali v drugi skrajnosti opišejo samo lastnosti oziroma obrambo pred napadi, ki jih sami štejejo kot največji doprinos predstavljenega protokola. Dodatna zmeda

nastane, ker avtorji nikoli ne opredelijo pomanjkljivosti ali ranljivosti svojih protokolov, tako da je težko razbrati, ali protokol ne vsebuje neomenjenih lastnosti in ali je ranljiv na neomenjene napade. V predstavljeni tabeli je to razvidno v več primerih, kjer so protokoli odporni na napredne napade, medtem ko najosnovnejše varnostne lastnosti sploh niso omenjene. V številnih raziskavah bi zato hevristična analiza varnosti lahko bila opravljena bolj celovito.

Protokoli vzpostavitve ključa z generiranjem skrivnega ključa in še posebej protokoli, ki delujejo na podlagi signala pospeškov, pogosto predpostavijo legitimnost naprav na telesu [181]. Isto velja tudi za protokole na osnovi fizioloških podatkov, vendar obstaja med obojimi pomembna razlika. Senzorska vozlišča s protokolom vzpostavitve ključa na osnovi fizioloških podatkov morajo biti za delovanje v stiku s telesom, kar bi uporabnik zelo težko spregledal. Nasprotno so lahko naprave s protokolom vzpostavitve ključa, ki deluje na podlagi signalov pospeška, nameščene kjer koli. Skupaj z razvojem senzorjev, ki omogoča, da so takšne naprave zelo majhne, je verjetnost, da bi napadalec uspešno namestil napravo na uporabnika (npr. podtaknil v žep), veliko večja. Takšna naprava bi zbirala enake podatke kot legitimna vozlišča v omrežju in se lahko posledično vključila v TSO. Druga potencialna pomanjkljivost uporabe signalov pospeška je pridobivanje teh vrednosti iz video nadzora uporabnika. Ta grožnja je bila izpostavljena v [176], vendar njena uporabnost ni bila nadalje raziskana.

Opravljen pregled literature, v kateri smo našli 116 protokolov za vzpostavitev ključa v TSO, je pokazal, da je za skoraj 77 % najdenih protokolov bila narejena vsaj ena oblika analize varnosti. Najpogostejša metoda vrednotenja najdenih protokolov je hevristična, ki je uporabljena v več kot 40 % vseh najdenih protokolov. Ta metoda je priljubljena predvsem pri vrednotenju tradicionalnih in hibridnih protokolov, medtem ko je veliko redkeje uporabljena za vrednotenje protokolov na osnovi fizioloških podatkov in protokolov z generiranjem skrivnega ključa. Od skupno 40 tradicionalnih protokolov, ki smo jih zasledili v literaturi, jih 29 (73 %) vključuje hevristično vrednotenje, od 17 hibridnih protokolov jih 10 (59 %) vsebuje hevristično vrednotenje, medtem ko je uporaba v protokolih na osnovi fizioloških podatkov in protokolih z generiranjem skrivnega ključa zgolj 22 % in 9 %. To pa ne pomeni, da članki, ki predstavijo protokole teh dveh oblik, ne vsebujejo analiz varnosti. Med pregledom literature smo našli 23 od skupno 36 (64 %) protokolov vzpostavitve ključa na osnovi fizioloških podatkov in 18 od skupno 23 (78 %) protokolov vzpostavitve ključa z generiranjem skrivnega ključa, ki so vsebovali vsaj eno obliko analize varnosti. Formalne in delno formalne metode vrednotenja se uporabljajo izredno redko. Med pregledom literature smo našli manj kot 9 % raziskav, ki so vsebovale vsaj eno od oblik formalnega ali delno formalnega vrednotenja varnosti predlaganih protokolov.

5.3 Metode vrednotenja učinkovitosti protokolov

Ena največjih razlik med TSO in tipičnimi omrežji so drastične omejitve strojne opreme, ki veljajo za senzorske naprave v TSO. Zato se v vseh elementih delovanja takšnih naprav

pričakuje minimalna poraba pomnilnika in računske moči ter čim manjša količina oddanih in prejetih podatkov ob uporabi čim manjšega števila sporočil, zato da se doseže čim manjša skupna poraba električne energije. Zaradi tako strogih omejitev strojnih virov in pomembnosti učinkovite izrabe teh virov se avtorji protokolov za vzpostavitev ključa v TSO pogosto odločajo za vključitev analize učinkovitosti predlaganih protokolov. Takšna analiza je pomembna za prikaz racionalne izrabe virov predstavljenega protokola oziroma za predstavitev učinkovitosti določenega protokola pred konkurenčnimi protokoli. Analiza učinkovitosti se pogosto deli na dele, namenjene pomnilniški, računski, komunikacijski in energijski učinkovitosti. Na podlagi pregleda metod vrednotenja učinkovitosti protokolov v literaturi bomo v nadaljevanju disertacije tudi sami analizirali učinkovitost predlaganih novih protokolov.

5.3.1 Učinkovitost porabe pomnilnika

Najpogostejša metoda, ki jo avtorji uporabljajo za merjenje učinkovitosti porabe pomnilnika, je v osnovi zelo preprosta – število bitov ali zlogov, ki jih mora naprava trajno hraniti za delovanje protokola [75, 80, 87, 90, 97, 103, 110, 113, 120, 121, 123–125, 138, 147, 157, 168, 188, 197, 199]. Drugi avtorji se odločijo za bolj nevtralen pristop, tako da predstavijo formulo, po kateri se lahko izračuna poraba pomnilnika za predlagani protokol. To omogoča prilagoditev porabe pomnilnika glede na uporabljene elemente v protokolu, ki bodo shranjeni v pomnilnik (velikost enkratnih vrednosti, velikost ključev, velikost izvlečka (odvisna od uporabljene zgoščevalne funkcije), število vozlišč v omrežju itd.). To omogoča preprost naknaden izračun porabe pomnilnika za različne kombinacije gradnikov. Takšna oblika vrednotenja učinkovitosti je bila uporabljena v raziskavah [117, 120, 123, 145, 151, 192, 196, 198]. Avtorji protokolov, kjer je protokol v veliki meri odvisen od predporazdeljenih ključev, uporabljajo kot metriko učinkovitosti protokola tudi število ključev, ki bodo trajno hranjeni na napravah [128, 160, 196].

Pri merjenju učinkovitosti porabe kateregakoli vira avtorji pogosto uporabijo primerjavo predlaganega protokola s podobnimi predhodno predstavljenimi protokoli. Če je izraba vira v novejšem protokolu učinkovitejša, je to zelo dober kazalnik skladnosti predlaganega protokola z omejitvami TSO. V primeru učinkovite uporabe pomnilnika se najpogosteje primerja količina zasedenega pomnilnika, kot so storili v naslednjih raziskavah [87, 107, 120, 130, 133, 151].

5.3.2 Računska zahtevnost

Naslednji pomemben kazalnik učinkovitosti je računska zahtevnost. Na senzorskih vozliščih v TSO je pomembno, da so protokoli računsko učinkoviti, saj so procesorske enote na takšnih napravah zelo preproste. Najpogostejša metrika, ki se uporablja za merjenje računske zahtevnosti, je čas izvajanja potrebnih računskih operacij, pri čemer daljše izvajanje predstavlja večji in/ali bolj zahteven nabor računskih operacij in tudi večjo porabo električne energije [72, 103, 109, 110, 116, 125, 126, 132, 138, 204]. Zato da se te vrednosti postavijo v

kontekst, avtorji pogosto primerjajo te čase s časi izvajanja drugih primerljivih protokolov [75, 80, 87, 90, 97, 98, 107, 117, 121, 123, 151, 193, 197]. Za lažje primerjanje računske zahtevnosti med protokoli se je uveljavila metoda primerjave na podlagi števila različnih računskih operacij (npr. zgoščevalna funkcija, šifriranje, generiranje ključa itd.), ki se izvedejo med vzpostavitvijo ključa. Takšna primerjava je lažja, saj ni odvisna od strojne opreme ali uporabljenih gradnikov (npr. uporaba različnih šifrirnih algoritmov ali zgoščevalnih funkcij). Metoda vrednotenja in/ali primerjave računske zahtevnosti na podlagi računskih operacij, vključenih v protokol, je uporabljena v [19, 20, 85, 90, 98, 104–106, 109, 115, 117, 123, 128, 133, 145, 147, 157, 198]. Na podlagi seznama vseh operacij in povprečnega trajanja posamezne operacije se pogosto ustvari tudi ocena trajanja izvajanja protokola (najpogostejša metoda vrednotenja računske zahtevnosti). Računska zahtevnost se pogosto izrazi tudi z računsko kompleksnostjo (angl. computational complexity), kjer je primerjava s sorodnimi protokoli ponovno zelo pogosta [84, 137, 144, 158, 160, 193]. Avtorji člankov [72, 120, 124, 168] merijo računsko zahtevnost na podlagi števila ciklov procesorja, ki so potrebni za izvedbo protokola. Poleg teh metod se računska zahtevnost v znanstvenih raziskavah, ki predlagajo nove protokole za vzpostavitev ključa v TSO, meri tudi s številom ključev, ki jih je potrebno generirati v protokolu [191], in z opisno primerjavo vseh operacij med predlaganim protokolom in drugimi predhodno predlaganimi protokoli [146]. V raziskavi [122] je analiza računske zahtevnosti opravljena na podlagi količine podatkov, ki morajo biti šifrirani. V protokolih vzpostavitve ključa z generiranjem skrivnega ključa je metoda merjenja časa tudi pogosta, vendar se v takšnih protokolih meri čas, potreben za generiranje ustreznih ključev [86, 113, 124, 199].

5.3.3 Učinkovitost komunikacije

Pošiljanje in prejemanje sporočil je energijsko najbolj zahtevna operacija, zato je pomembno, da protokol za vzpostavitev ključa v TSO pošilja in prejema čim manjše količine podatkov [70]. Posledično je tudi najpogosteje uporabljena metrika za vrednotenje učinkovitosti komunikacije količina poslanih podatkov [72, 75, 80, 87, 90, 120–123, 127, 128, 133, 146, 159, 194]. Preprostejša oblika merjenja poslanih podatkov je s številom sporočil, ki so poslana [19, 84, 87, 105, 106, 191]. Tako kot pri prejšnjih kazalnikih učinkovitosti se tudi pri učinkovitosti komunikacije avtorji pogosto odločijo za primerjavo z drugimi protokoli za vzpostavitev ključa v TSO. Primerjave na podlagi prenesenih bitov so bile narejene v [87, 97, 107, 117, 128, 135, 157], medtem ko naslednje raziskave vsebujejo primerjavo na podlagi števila poslanih sporočil [87, 119, 160, 191, 192, 196]. Alternativni načini merjenja učinkovitosti komunikacije so zelo redki. Avtorji članka [160] analizirajo pogostost potrebe po zamenjavi ključa, ki je glavni delež prenesenih podatkov v predlaganem protokolu vzpostavitve ključa. Avtorji člankov [139, 151] uporabijo opisno metodo, medtem ko se v raziskavah [122, 195] kompleksnost komunikacije opredeli kot količina energije, ki bo porabljena za namen prenosa podatkov med izvajanjem protokola vzpostavitve ključa.

5.3.4 Učinkovitost porabe energije

Zadnji pogost kazalnik učinkovitosti protokola je poraba energije. Učinkovita izraba energije vključuje tudi prejšnja kazalnika učinkovitosti, saj njihova učinkovitost vpliva na končno porabo energije. Velika večina avtorjev poda porabo energije v joulih (J) [71, 72, 74, 75, 87, 90, 111, 116, 117, 119, 121–123, 126, 128, 133, 135, 139, 145, 159, 160, 188, 192, 194–197]. Nekatere od teh vrednosti so bile pridobljene z merjenjem prototipnih implementacij, medtem ko so druge nastale na podlagi predhodnih raziskav, v katerih so bile podane vrednosti porabe specifičnih naprav ob izvajanju specifičnih operacij, na podlagi katerih lahko avtorji novih protokolov ocenijo njihovo porabo energije (primera takšnega vrednotenja porabe energije sta [122, 195]). Zasledili smo tudi raziskave, kjer se je poraba električne energije merila glede na vsak bit informacij, ki je generiran [112], in primer, kjer se poraba meri v amperurah (Ah; angl. ampere-hours) [124].

Kot je bilo omenjeno, so nekateri avtorji svoje protokole tudi implementirali. S tem lahko merijo porabo energije kot tudi čas izvajanja, ki je, kot smo prej omenili, najpogostejši način merjenja računske zahtevnosti. Za implementacijo protokolov se avtorji poslužujejo različnih naprav in simulatorjev, od katerih so odvisne tudi pridobljene meritve. Posledično rezultati analiz učinkovitosti porabe energije in računske zahtevnosti različnih protokolov niso vedno primerljivi. Tu smo zbrali nekaj podatkov o različni strojni opremi, uporabljeni v različnih analizah. Te naprave niso prilagojene za delovanje v TSO, ampak so tipično večnamenski mikrokrmilniki (angl. microcontroller), pogosto pa je v člankih navedena zgolj centralno procesna enota: MicaZ [87, 117, 120, 124, 197], Mica2 [140, 187], Tmote-Sky [86, 103, 113, 116, 117], Arduino Uno [118], Raspberry PI 2 [109], Waspmote [98], Chipcon CC2420 [145], AquisGrain 2 [125], TelosB [74, 126, 138, 197], Sun SPOT [121], MSP430 [72], Cortex-M3 [75, 123, 199], PXA270 [75] in SHIMMER [110].

5.3.5 Vrednotenje učinkovitosti protokolov vzpostavitve ključa na osnovi fizioloških podatkov

Tako kot pri vrednotenju varnosti ima tudi vrednotenje učinkovitosti protokolov na osnovi fizioloških podatkov določene specifičnosti. Analize učinkovitosti takšnih protokolov se osredotočajo predvsem na pridobivanje vrednosti iz fizioloških signalov. Pri pridobivanju skrivnih vrednosti iz signala so pomembne naključnost (angl. randomness), razlikovalnost (angl. distinctiveness), časovna varianca (angl. temporal variance) in latenca (angl. latency) za pridobitev skrivne vrednosti. Naključnost generiranih vrednosti je vrednotena na podlagi entropije ustvarjene vrednosti in v osnovi predstavlja verjetnost, da je ustvarjena specifična vrednost [196]. V idealnem primeru imajo vse vrednosti enako verjetnost, da so ustvarjene, in njihovo zaporedje ni predvidljivo [158]. Razlikovalnost je pomembna, ker pove, ali so fiziološki signali in posledično generirane vrednosti dovolj raznolike, da je na njihovi podlagi mogoče razlikovati med uporabniki [77]. To preprečuje generiranje enakih vrednosti na različnih uporabnikih in zagotavlja, da se bodo samo vozlišča v istem omrežju lahko uspešno overila

med seboj [129]. Časovna varianca oziroma ponovljivost generiranih vrednosti je pomembna za preprečevanje ponavljanja generiranih vrednosti, ustvarjenih iz ponovljivega merjenja fiziološkega signala [136]. To zagotavlja, da odkritje fiziološkega signala ne ogrozi varnosti v preteklosti ali v prihodnosti generiranih vrednosti [128]. Latenca je podatek o potrebnem času merjenja signala, zato da je zbranih dovolj podatkov za generiranje varne skrivne vrednosti. Nižja latenca je boljša, ker lahko tako hitreje generiramo naključne vrednosti. Tu je seznam vseh raziskav predlaganih protokolov, v katerih se analizira vsaj nekaj od teh lastnosti [77, 128, 129, 132, 136–138, 140, 147, 151, 158, 160, 190, 193, 196, 198]. Skoraj vsi avtorji uvrščajo te lastnosti v analizo učinkovitosti, vendar te iste lastnosti istočasno pokažejo tudi varnost protokola oziroma generiranih vrednosti v protokolu, zato bi lahko te lastnosti uvrstili tudi v analizo varnosti (podobno kot ocena entropije v primeru varnostne analize protokolov vzpostavitve ključa z generiranjem skrivnega ključa).

Drugi metriki, ki se pogosto uporabljata za vrednotenje učinkovitosti protokolov na osnovi fizioloških podatkov, sta stopnja napačne odobritve (angl. false acceptance rate – FAR) in stopnja napačne zavrnitve (angl. false rejection rate – FRR). Metriki sta namenjeni merjenju uspešnosti overjanja in sta tipični metodi vrednotenja biometričnih sistemov. Obe metriki sta namenjeni prikazovanju uspešnosti sistema pri razlikovanju med istimi in različnimi biometričnimi podatki. Stopnja napačne odobritve je pogostost, s katero se nepooblaščenemu uporabniku odobri dostop (vozlišči v ločenih TSO se uspešno overita oziroma izmenjata ključ). Stopnja napačne zavrnitve je pogostost, s katero je veljavnemu uporabniku zavrnjen dostop (vozlišči na istem telesu ob merjenju istega fiziološkega signala ne proizvedeta primerljivih vrednosti, s katerimi bi se lahko overili oziroma vzpostavili ključ). Raziskave so pokazale, da sta si metriki obratno sorazmerni. To pomeni, da se z znižanjem ene metrike druga poveča. S spreminjanjem števila lastnosti, ki se pridobijo iz signala, je možno vplivati na metrike. Z upoštevanjem obeh lastnosti morajo avtorji protokolov zagotoviti primerno ravnovesje med stopnjama napačnih odobritev in napačnih zavrnitev. Polovična napaka verifikacije (angl. half total error rate – HTER) je metrika, ki združuje stopnjo napačne odobritve in stopnjo napačne zavrnitve. Nižja kot je vrednost polovične napake verifikacije, boljša je povprečna vrednost obeh metrik, ki jo sestavljata. Predstavljene metrike so uporabljene v naslednjih raziskavah [15, 60, 74, 77, 129, 130, 132, 133, 139, 140, 142, 144–147, 150–153, 155, 159, 161, 169, 194, 198].

Metode vrednotenja učinkovitosti, predstavljene v tem poglavju, so uporabljene predvsem za vrednotenje protokolov vzpostavitve ključa na osnovi fizioloških podatkov, vendar se uporabljajo tudi v hibridnih protokolih (kjer so tudi prisotni fiziološki podatki) in izjemoma tudi v protokolih z generiranjem skrivnega ključa, ki so v določenih pogledih zelo podobni protokolom na osnovi fizioloških podatkov. Zato so v tem poglavju prisotne tudi reference na protokole iz teh dveh skupin.

5.3.6 Vrednotenje učinkovitosti protokolov vzpostavitve ključa z generiranjem skrivnega ključa

Vrednotenje učinkovitosti protokolov z generiranjem skrivnega ključa se v znanstveni literaturi opravi na dva načina. Usklajenost ključev (angl. key agreement; v angleščini je poimenovanje enako dogovoru o ključu) meri delež skladnih bitov ključa, ki so jih generirale neodvisne naprave. Če je ustvarjeni ključ enak na vseh napravah v procesu vzpostavitve ključa, potem je usklajenost ključa 100 %. Ta metrika torej oceni verjetnost, da bodo naprave uspešno vzpostavile skupen skrivni ključ. Usklajenost ključa, ki ga generira napadalec, bi morala biti približno 50 % (enako kot za naključno ustvarjeno zaporedje bitov). Druga metrika je hitrost generiranja skrivnih bitov (angl. secret bit rate). Hitrost generiranja skrivnih bitov pove, koliko bitov ključa je generiranih iz danega signala v določeni časovni enoti. Na to hitrost vplivajo hitrost vzorčenja, metoda kvantizacije, njeni parametri in variabilnost signala (npr. protokoli, ki temeljijo na indikatorju moči sprejetega signala ali signalih pospeška, imajo višjo hitrost generiranja skrivnih bitov, ko je uporabnik v gibanju). Cilj je razviti protokole z visoko usklajenostjo ključev in visoko hitrostjo generiranja skrivnih bitov, vendar si ti cilji nasprotujejo. Hitrejše vzorčenje meri manj variabilnosti signala, kar vodi v slabšo usklajenost ključev in tudi nižjo entropijo. Obratno drži za počasnejše vzorčenje. Naslednje raziskave vključujejo analizo učinkovitosti predlaganih protokolov z generiranjem skrivnih ključev z metrikami usklajenosti ključa in/ali hitrosti generiranja skrivnih bitov [74, 162–168, 170–177, 179–185]. Pri takšnih vrstah analize učinkovitosti je potrebno biti pozoren na dejstvo, da so rezultati, na podlagi katerih so protokoli ocenjeni, pridobljeni z merjenjem eksperimentalnih implementacij, ki so jih razvili in izvedli avtorji protokolov. Rezultati analize so zato odvisni od okoliščin eksperimenta (npr. kje na telesu je nameščena naprava, kakšne premike opravlja uporabnik ob zajemanju signalov itd.), zato se primerljivost med analizami različnih protokolov in ponovljivost eksperimenta lahko izkrivita.

5.4 Razprava o vrednotenju učinkovitosti protokolov za vzpostavitev ključa v TSO

Najbolj primeren način vrednotenja učinkovitosti protokolov za vzpostavitev ključa v TSO je način, ki ni odvisen od spremenljivih dejavnikov. Pri merjenju učinkovitosti porabe pomnilniškega prostora je najpogostejša uporabljena metrika količina pomnilnika, ki ga protokol potrebuje. To je dobra metrika, ker so rezultati razumljivi in lahko primerljivi med različnimi protokoli, vendar so vezani na uporabo specifičnih kriptografskih elementov (npr. zgoščevalna funkcija, velikost ključev itd.). Varnost protokolov ni vezana na uporabo točno določenih elementov, dokler ti elementi izpolnjujejo potrebne varnostne lastnosti, zato se v protokolih ti nikoli ne določijo (dokler niso standardizirani). Posledično je protokole možno implementirati z uporabo različnih kriptografskih elementov, kar lahko izrazito spremeni količino podatkov, ki jih protokol hrani. Iz teh razlogov je boljša takšna metrika, ki upošteva

možne spremembe. Zato je metoda identifikacije vseh elementov, ki bodo trajno hranjeni na pomnilniku, dobra izbira. Iz takšnega seznama je še vedno možno izračunati pomnilniško učinkovitost protokola ob uporabi tipičnega/lastnega nabora kriptografskih gradnikov in podati rezultat v bolj razumljivi obliki (bitih ali zlogih).

Računska zahtevnost je vrednotena predvsem z metriko časa izvajanja in metriko identifikacije vseh računskih operacij v protokolu. Časovna zahtevnost je v veliki meri odvisna od strojne opreme, na kateri se protokol testira. Kot smo pokazali v poglavju 5.3.4, na področju ne obstaja določena strojna oprema, ki bi se uporabljala pri testiranju vseh protokolov, zato je primerjava rezultatov protokolov, ki so testirani na različnih napravah, lahko zavajajoča. Način merjenja računske zahtevnosti, ki odstrani to težavo, je identifikacija vseh računskih operacij in primerjava med več protokoli glede na razlike med vrsto in številom posameznih operacij. Tako je vsaj za namene primerjave druga možnost vrednotenja računske zahtevnosti veliko bolj prijazna, čeprav to še vedno ni popoln način. Da lahko na takšen način primerjamo protokole, morajo biti ti dokaj podobni. Če vsebujejo različne vrste operacij (npr. šifrirni algoritem ali zgoščevalna funkcija) ali definirajo algoritme z različno računsko kompleksnostjo (npr. AES in Twofish), postane primerjava med njimi ponovno brezpredmetna, če ne obstaja nobena raziskava o primerjavi računske zahtevnosti takšnih operacij.

Učinkovitost komunikacije se v literaturi skoraj izključno vrednoti na podlagi količine podatkov in števila sporočil, ki se prenesejo med procesom vzpostavitve ključa. Količina podatkov neposredno vpliva na količino energije, ki jo operacija potroši, medtem ko večje število manjših sporočil povzroči več režijskih stroškov, kar ponovno poveča porabo električne energije. Metriki sta neodvisni ena od druge, zato bi bila dobra praksa v analizo učinkovitosti komunikacije vključiti obe, čeprav rezultati pregleda literature iz poglavja 5.3.3 kažejo, da se avtorji redko odločijo za to.

Zadnji splošen kazalnik učinkovitosti protokola je energijska učinkovitost. Ta je v veliki večini odvisna od računskih operacij in komunikacije naprave, zato je učinkovitost izrabe energije kroven kazalnik učinkovitosti celotnega protokola. Poraba električne energije je merjena na testnih implementacijah ali na podlagi predhodnih ocen porabe specifične operacije na določeni napravi, toda ker med raziskovalci ni soglasja o strojni opremi, na kateri testirati protokole, so rezultati redko primerljivi. Trenutno ne obstaja rešitev za to težavo, v prihodnosti pa bi se lahko opravile raziskave na temo porabe energije v najbolj pogosto uporabljenih testnih napravah za TSO. Rezultati takšnih raziskav bi olajšali razvijalcem vrednotenje bodočih protokolov in omogočili primerjavo že obstoječih protokolov, ki so bili testirani na različni strojni opremi.

Od skupno 116 člankov, vključenih v pregled literature, smo analizo vsaj enega od teh štirih kazalnikov učinkovitosti protokola zasledili v 57 % primerov, medtem ko je kakršno koli obliko analize učinkovitosti (protokoli na osnovi fizioloških podatkov in protokoli z generiranjem skrivnega ključa pogosto ne vključujejo osnovnih štirih kazalnikov učinkovitosti) vsebovalo kar 86 % vključenih člankov. Če spomnimo, je varnostno analizo vsebovalo samo 77 % vseh člankov, kar bi lahko nakazovalo, da med glavnima karakteristikama TSO (tj.

varovanje občutljivih informacij, ki se pošiljajo preko takšnih omrežij, in omejitve virov, ki so prisotne na napravah v takšnih omrežjih) raziskovalci posvetijo več svoje pozornosti zagotavljanju učinkovitosti izdelanih protokolov, kot je namenijo preverjanju varnostnih karakteristik.

5.5 Izbor metod za ocenjevanje varnosti in učinkovitosti novo razvitih protokolov

Cilj disertacije je razvoj novega protokola za vzpostavitev ključa, primernega za uporabo v TSO. Kot je bilo predstavljeno, je pomemben del opisa novih protokolov dokaz njihovega varnega delovanja in učinkovitosti izrabe omejenih virov. V 5. poglavju smo naredili pregled vseh metod vrednotenja varnosti in različnih kazalnikov učinkovitosti, uporabljenih v znanstveni literaturi na področju protokolov vzpostavitve ključa v TSO. Pokazano je bilo, da so nekatere metode veliko pogosteje uporabljene. Za metode vrednotenja istega kazalnika učinkovitosti so bile predstavljene prednosti oziroma slabosti posameznega pristopa. Te zbrane informacije bodo v nadaljevanju uporabljene za namene preverjanja varnostnih lastnosti in učinkovitosti delovanja protokolov, razvitih v tej disertaciji. To podpoglavje je namenjeno razlagi izbora metod vrednotenja varnosti in učinkovitosti, ki ga bomo v nadaljevanju uporabili za vrednotenje lastnih protokolov.

V nadaljevanju disertacije bosta predstavljena dva nova protokola. Oba sodita med tradicionalne protokole, zato bodo za njuno analizo uporabljene metode, ki se praviloma uporabljajo v takšnih protokolih.

Prvi novi protokol – protokol I – je zelo podoben predhodnemu protokolu, ki ga izboljšuje. Zato sta analiza varnosti in analiza učinkovitosti ustvarjeni na podlagi analize originalnega protokola. Analiza varnosti bo opravljena s hevristično metodo, ki je bila uporabljena tudi v analizi predhodnega protokola. V analizi učinkovitosti protokola I bo najprej nekaj besed namenjenih analizi predhodnega protokola. To je potrebno, ker ta vključuje določene nepravilnosti glede vrednotenja zahtevnosti računskih operacij, uporabljenih v protokolu. Po predstavljenih popravkih teh ocen računske zahtevnosti bo preostanek analize namenjen vrednotenju računske zahtevnosti, učinkovitosti komunikacije in učinkovitosti porabe energije protokola I. Novi protokol I ima identične pomnilniške zahteve kot protokol, katerega delovanje izboljšuje, zato je bila ta metrika vrednotenja učinkovitosti izpuščena. Vključena je tudi primerjava obeh protokolov, ki je, kot smo videli v pregledu literature, tudi zelo pogosta metoda analize učinkovitosti.

Drugi novi protokol za vzpostavitev ključa v TSO – protokol II – bo tako kot protokol I varnostno analiziran z v literaturi najpogosteje uporabljeno hevristično metodo. V analizi bodo upoštevane vse varnostne lastnosti in odpornosti na napade, ki so bili predstavljeni v poglavjih 4.1 in 4.2. V analizo učinkovitosti bodo vključene učinkovitost porabe pomnilnika, računska zahtevnost in učinkovitost komunikacije. Uporabljene bodo metode vrednotenja, ki so

neodvisne od okoliščin meritev. Skupno oceno učinkovitosti porabe električne energije bi zato bilo možno izdelati s pomočjo teh metrik in ob uporabi ocen ali meritev porabe energije posameznih elementov protokola. Ker je pregled literature pokazal, da so primerjave med protokoli v analizi učinkovitosti zelo pogoste, bo protokol II tudi primerjan z dvema sorodnima protokoloma.

6 Izboljšani protokol za overjanje in vzpostavitev ključa v telesnih senzorskih omrežjih

V tem poglavju je predstavljen nov protokol za vzpostavitev ključa v TSO, ki je izboljšava obstoječega protokola, ki sta ga predstavila M.R. Abdmeziem in D. Tandjaoui [122]. Oba protokola spadata med tradicionalne protokole in omogočata varen transport ključa od senzorskih naprav do strežnika v zdravstveni ustanovi, ki hrani zbrane podatke in nadzira dostop do njih. Osnovna ideja originalnega protokola je preoblikovanje protokola, ki varuje prenos ustvarjenih ključev s pomočjo asimetričnega para ključev, na takšen način, da se zahtevne operacije asimetrične kriptografije iz senzorskih vozlišč premaknejo na strojno neomejene naprave. Vzpostavitev ključa in varovanje komunikacije med senzorskim vozliščem in dodanimi tretjimi entitetami se opravi na nezahteven način, ki je bolj primeren za uporabo na manj zmogljivih napravah. V nastalem protokolu senzorska vozlišča, ki delujejo na telesu uporabnika, vzpostavijo varovano komunikacijo s strežnikom v zdravstvenem centru preko tretjih entitet, ki posredujejo skrivnost od senzorskih vozlišč do strežnika. Izboljšani protokol zagotavlja večjo varnost brez izrazitega povečanja porabe virov. V nadaljevanju bomo izboljšani protokol imenovali protokol I.

Rezultati tega poglavja, vključno z analizo originalnega protokola, predstavitvijo izboljšanega protokola in analizo njegove varnosti in učinkovitosti, so bili povzeti po objavljenem članku z naslovom *Analysis and improvement of a secure key management protocol for e-health applications* [205] v reviji *Computers & Electrical Engineering*.

V nadaljevanju tega poglavja bomo uporabljali številne okrajšave deležnikov in vrednosti, ki so prisotne v originalnem in izboljšanem protokolu. Seznam uporabljenih okrajšav oziroma simbolov skupaj z opisom njihovih pomenov je v naslednji tabeli (Tabela 6.1).

Tabela 6.1: Definicija okrajšav, uporabljenih v poglavju 6.

Simbol	**Opis**
V	(Senzorsko) vozlišče
Z	Strežnik v zdravstvenem centru, ki zbira podatke in ureja dostop do njih
TE_i	Tretja entiteta (i-ta v vrsti)
VP	Varnostna politika
N_X	Enkratna vrednost (angl. nonce), ki jo je ustvaril X
$N_{X,Y}$	Enkratna vrednost, ki jo je ustvaril X, z namenom deljenja z Y
$K_{X,Y}$	Simetrični ključ, deljen med X in Y
K_X	Javni ključ entitete X

S	Skrivnost, ki jo ustvari V in posreduje Z in iz katere se ustvari sejni ključ
S_i	Del skrivnosti S (i-ti del)
O_i	Vrednost, ki določi položaj S_i v celotni skrivnosti S
$[Podatki]_K$	Podatki, šifrirani s ključem K
$h(X)$	Zgoščena vrednost (angl. hash) vrednosti X (kjer X predstavlja več vrednosti, so te vrednosti združene z operacijo spajanja)
$SIGN_X$	Digitalni podpis entitete X

6.1 Protokol Abdmeziem-Tandjaoui in njegove pomanjkljivosti

M.R. Abdmeziem in D. Tandjaoui sta predlagala protokol vzpostavitve ključa [122] med vozliščem z omejenimi strojnimi viri in oddaljeno napravo (strežnik v zdravstvenem centru) na osnovi prelaganja računsko zahtevnih operacij (asimetrična kriptografija) z manj zmogljivih naprav na druge naprave, ki nimajo strogih strojnih omejitev. Te tretje entitete so sposobne opravljanja prenesenih operacij in so overjene, čeprav niso nujno zaupanja vredne. Tretje entitete so naprave, ki jih lastniki prostovoljno vključijo v sistem preko katerega postanejo posredniki v protokolu vzpostavitve ključa. Oddaljeni strežnik hrani in opravi potrebno nadaljnjo obdelavo prejetih podatkov. Poleg omenjenih treh najpomembnejših entitet vzpostavitve ključa je v sistemu prisoten tudi overitelj potrdil, ki omogoča overjanje strežnika in tretjih entitet. V komunikaciji med senzorskimi napravami in tretjimi entitetami je tipično prisoten tudi osebni strežnik, ki v tem protokolu zgolj posreduje sporočila med naslovniki, zato v opisu protokola ni omenjen.

Tako kot velika večina tradicionalnih protokolov s predporazdeljenimi vrednostmi se tudi ta protokol začne z inicializacijsko fazo, v kateri je na vsako vozlišče (V) nameščen seznam tretjih entitet (TE), ki jih lahko V vpraša za sodelovanje pri vzpostavitvi ključa. Za vsako TE prejme V tudi predporazdeljen simetrični ključ (K_{V,TE_i}). Ti podatki so nameščeni na naprave preko varnega kanala, kjer prisluškovanje ni mogoče. Sam protokol vzpostavitve ključa je nadalje razdeljen v pet faz. Vse faze in posamezna sporočila, poslana v protokolu, so prikazani na sliki, ki sledi predstavitvi posameznih faz protokola (Slika 6.1). Ob desnem robu slike so označbe posameznih sporočil (A–K) in ob levem robu so označene faze protokola (faza 1–5).

Faza 1 se začne, ko želi V vzpostaviti povezavo s strežnikom v zdravstvenem centru (Z). To stori s pozdravnim sporočilom V_HELLO, ki vključuje podatke o možnih varnostnih politikah (uporabljen šifrirni algoritem, trajanje veljavnosti sejnega ključa itd.). Na to sporočilo Z odgovori z lastnim pozdravnim sporočilom Z_HELLLO, ki vsebuje izbrano varnostno politiko. Obe sporočili (sporočili A in B) vključujeta tudi enkratno vrednost (N_V in N_Z) za preprečevanje napada s ponavljanjem sporočil.

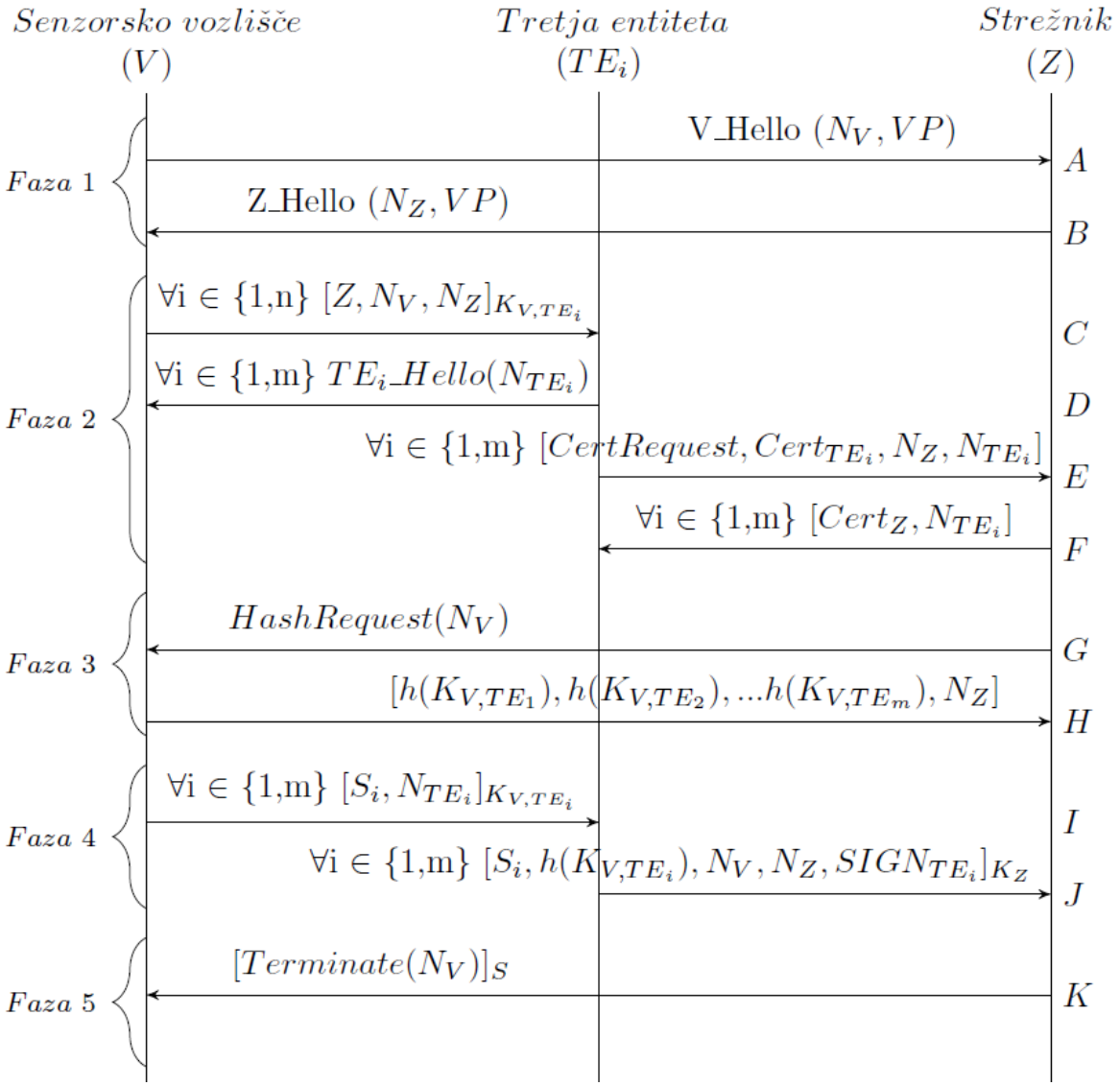
Faza 2 je namenjena vpeljavi TE v komunikacijo. V sporočilu C pošlje V identiteto Z in v prejšnjih sporočilih vzpostavljena N_V ter N_Z vsem TE, ki jih ima v predporazdeljenem seznamu. Ta sporočila so šifrirana s pripadajočim K_{V,TE_i}. Avtorji priporočajo uporabo načina

šifriranja AES-CCM [206], ki omogoča uporabo istega ključa za šifriranje in istočasno izdelavo kode za overjanje sporočila. Po prejetju sporočila se vsaka TE odloči, ali želi sodelovati v procesu vzpostavitve ključa med V in Z. TE_i se lahko iz različnih razlogov odloči in ne sodeluje v protokolu vzpostavitve ključa (npr. zasedenost ali pretečena veljavnost certifikata). Če je n število TE, ki jim je V poslalo sporočilo C, je m število sprejetih prošenj, tako da je $m \leq n$. TE, ki želijo sodelovati, pošljejo nazaj TE_i_HELLO sporočilo z lastno enkratno vrednostjo (N_{TE_i}). Takoj zatem lahko TE pošljejo zahtevo Z po certifikatu, ki vključuje lasten certifikat TE_i, N_{TE_i} ter N_V. Strežnik Z odgovori na zahtevo in v sporočilo vključi prejeto enkratno vrednost (N_{TE_i}) z namenom preprečevanja napada s ponavljanjem. Posredovani certifikati se preverijo pri organu za preverjanje veljavnosti potrdil.

Faza 3 je namenjena dokazovanju, da TE_i, od katerih je Z prejel sporočila, zastopajo interese V. Potem ko Z odgovori na vse zahteve po certifikatu, pošlje vozlišču V zahtevo po zgoščenih vrednostih ($HashRequest$; sporočilo G). Ta zahteva naj bi vključevala seznam vseh TE_i, za katere želi Z pridobiti zgoščene vrednosti, čeprav tega avtorji niso vključili v diagram izmenjave sporočil. V odgovori s seznamom simetričnih gesel, ki si jih deli s TE, ki so sprejele prošnjo po sodelovanju pri vzpostavitvi ključa. Vsak ključ je v seznam zapisan v zgoščeni obliki ($h(K_{V,TE_i})$). S pomočjo teh vrednosti bo kasneje Z potrdil, da so naprave, ki so od njega zahtevale certifikat, bile kontaktirane s strani V in jim je ta predal veljaven del skrivnosti S. Kot vedno obe sporočili vsebujeta enkratne vrednosti.

Faza 4 je namenjena posredovanju S od V preko TE do Z. Vozlišče V ustvari S ter jo razdeli na m delov – število TE, ki sodelujejo v protokolu. Vsak del skrivnosti (S_i) je zatem posredovan posameznim TE_i v šifriranem sporočilu I. Sporočilo vključuje tudi enkratno vrednost in je šifrirano s predporazdeljenim ključem K_{V,TE_i}. Vsak TE_i po prejemu sporočila to dešifrira in pridobljeno vrednost S_i vstavi v novo sporočilo J. V sporočilu sta vključeni še dve enkratni vrednosti, zgoščena vrednost predporazdeljenega simetričnega ključa ($h(K_{V,TE_i})$) in digitalni podpis vseh vrednosti. Sporočilo je šifrirano z javnim ključem strežnika (K_Z). Ko Z prejme sporočilo od posamezne TE_i, ga najprej dešifrira, nato preveri podpis in nazadnje preveri, da je bila prejeta vrednost $h(K_{V,TE_i})$ vključena v odgovor V na zahtevo po zgoščenih vrednostih (sporočilo H). S tem se T prepriča, da vsi TE_i zastopajo V. Po prejetju vseh sporočil lahko Z iz vseh S_i ponovno sestavi prvotno S. Skrivnost S bo uporabljena za izdelavo sejnega ključa.

Faza 5 je zadnja faza protokola. V zadnjem sporočilu Z šifrira N_V z ravnokar pridobljeno skrivnostjo S. S tem ko V uspešno dešifrira to sporočilo, je Z dokazal, da pozna skrivnost S.



Slika 6.1: Izmenjava sporočil v protokolu Abdmeziem-Tandjaoui [122].

6.1.1 Analiza delovanja protokola Abdmeziem-Tandjaoui

Protokol Abdmeziem-Tandjaoui predstavlja idejo prelaganja zahtevnih računskih operacij s strojno omejenih naprav na naprave, ki takšnih omejitev nimajo. Takšna zasnova delovanja protokola za overjanje in vzpostavitev ključa v TSO ni bila nikdar pred tem uporabljena. Tudi iz tega razloga so v protokolu prisotne določene pomanjkljivosti, ki lahko izhajajo iz same zasnove delovanja ali pa so posledica dotičnega protokola. Oboje bomo želeli odpraviti v izboljšanem protokolu I ali pa nanje vsaj opozoriti oziroma podati potencialne rešitve.

Za začetek izpostavimo dobre lastnosti protokola Abdmeziem-Tandjaoui oziroma načina delovanja vzpostavitve ključa s prenosom računsko zahtevnih operacij z manj zmogljivih naprav *V* na tretje entitete *TE*, ki nimajo težav z izvajanjem takšnih operacij. Na prvi pogled je prednost takšnega delovanja očitna. V disertaciji smo že veliko govorili o tem, kako je

asimetrična kriptografija neprimerna za uporabo na senzorskih napravah v TSO, tudi ko gre za KEK. Predlagana ideja odstrani takšne operacije s teh naprav in posledica je veliko učinkovitejše delovanje senzorskih naprav, kar je zagotovo dobra lastnost predlaganega načina delovanja. Na V se uporaba asimetrične kriptografije nadomesti s predporazdeljenim simetričnim ključem za vsako TE_i v ravno tako predporazdeljenem seznamu vozlišč. Uporaba predporazdeljenega trajnega ključa, ki ga ni mogoče dinamično spremeniti brez dostopa do naprave, ima resno pomanjkljivost. V primeru razkritja trajnega ključa bo ta razkrit, dokler se ga ne spremeni na napravi. To je težava, če razkritje ni znano, oziroma je posebej nezaželeno v primeru vgrajenih naprav. Prva resna pomanjkljivost uporabe predporazdeljenega simetričnega ključa je torej odpoved varne komunikacije, potem ko je ključ razkrit. Druga dobro poznana pomanjkljivost je slaba razširljivost. Obe pomanjkljivosti uporabe predporazdeljenih ključev sta v protokolu Abdmeziem-Tandjaoui izboljšani. Razširljivost oziroma dodajanje nove naprave v omrežje ni težava, saj napravam, ki so že vključene v omrežje, ni treba dodati novega simetričnega ključa za komunikacijo s to napravo. Ključ je potrebno dodati na določene TE, kar pa je možno storiti na varen in oddaljen način. Dodatna prednost je, da lahko imajo naprave, ki se nahajajo na istem telesu, različne sezname TE, kar preprečuje globalnim napadalcem, da bi na enostaven način zgradili seznam naprav v istem TSO. Problematika razkritja predporazdeljenega ključa je v protokolu Abdmeziem-Tandjaoui naslovljena na dva načina. Prvi je preprosto večje število TE, kar omogoča, da je tudi v primeru razkritja enega od simetričnih ključev končna skrivnost še vedno varna, ker je posredovana preko večjega števila TE in je razkrit samo majhen delček te skrivnosti. V primeru kompromitiranega vozlišča, ko se razkrijejo vsa gesla naprave, pa to še vedno predstavlja resno grožnjo (temu problemu se je nemogoče izogniti ob uporabi trajnih skrivnosti). Drugi način, s katerim prelaganje zahtevnih operacij izboljša pomanjkljivosti uporabe predporazdeljenih ključev, je ukinitev ene same naprave, ki pozna vse trajne ključe. Tradicionalno ima v takšnem sistemu vsak odjemalec ključ deljen s strežnikom, ki hrani ključe vseh uporabnikov. Strežnik je zato veliko večja tarča napadalcev, ker v primeru uspešnega napada napadalec pridobi ključe vseh uporabnikov, medtem ko je napad na vsakega posameznega odjemalca prezahteven oziroma neučinkovit. V protokolu Abdmeziem-Tandjaoui se koncentracija hranjenih ključev razporedi z enega strežnika na poljubno veliko število TE. Zato da lahko napadalec pridobi skrivnost, ki se vzpostavi med V in Z, bi moral pridobiti dostop do vseh TE, ki so v seznamu vozlišča V, kar je veliko težje, kot če napadalec ve točno, katero napravo mora napasti, da pridobi vse hranjene ključe (ogrozi varnost vseh uporabnikov), in je ta naprava samo ena. V primeru razkritja zasebnega ključa Z se lahko ta brez posledic za uporabnike hitro in preprosto menja. Če torej povzamemo doprinos protokola Abdmeziem-Tandjaoui, ta občutno zmanjša potrebne računske operacije na senzorskih napravah in istočasno odstrani oziroma omili glavne pomanjkljivosti uporabe trajnih predporazdeljenih ključev.

Z razdelitvijo procesa vzpostavitve ključa na dva ločena dela (en del je med V in TE_i ter drugi del med TE_i in Z) se splošna varnost protokola zmanjša, saj ima s tem napadalec dve različni obliki delovanja, ki ju lahko napade. Več možnosti napada je vedno v korist napadalcu, saj mora biti uspešen samo na enem delu, da izniči varnost celotnega protokola. Ne glede na to

pomanjkljivost v konceptu prelaganja zahtevnih operacij je to razumljiv kompromis glede na omejitve, ki so prisotne v TSO. S to delitvijo protokola se med obema polovicama ustvari tudi območje, v katerem je posredovana skrivnost oziroma njeni deli (S_i) nezavarovana, preden jih TE_i ponovno šifrirajo z naslovnikovim javnim ključem. To pomeni, da protokol ni varen od konca do konca (angl. end-to-end secure), saj se vsak del skrivnosti med prenosom razkrije (četudi samo overjenim entitetam). Po definiciji takšnega delovanja [207] deluje protokol od konca do konca samo na končnih napravah (protokol se ne izvaja na vmesnih točkah).

Razdelitev komunikacije na dva sklopa razdeli tudi overjanje na dva ločena dela. Vozlišče V ve, da komunicira s TE_i, in Z ve, da komunicira s TE_i, vendar obe končni napravi ne moreta biti prepričani, da komunicirata z isto vmesno tretjo entiteto. V tej točki je zato mogoča oblika napada pooseblјanja. Potem ko TE_i prejme prošnjo za sodelovanje pri vzpostavitvi ključa, lahko ta posreduje prejete podatke drugi napravi, ki lahko ni v seznamu TE na V. Druga naprava se lahko s temi podatki (in če ima ustrezen certifikat) zatem overi in poveže na Z. V nadaljevanju posreduje TE_i drugi entiteti tudi del skrivnosti, ki jo je TE_i pridobil od V. Na takšen način se je uspešno zaključil prenos ključa, čeprav se naprava, ki jo je kontaktiralo V, ni nikoli overila pri Z. Takšno delovanje lahko napadalec izkoristi in preusmerja komunikacijo z naprav, ki so izgubile veljavnost certifikata, ker so se izkazale za zlonamerne ali ker jim je preprosto potekla veljavnost certifikata, na TE, katerih nadzor je napadalec prevzel oziroma še niso bile razkrite kot zlonamerne in so pod njegovo kontrolo. To je mogoče tudi zato, ker se predporazdeljen seznam TE na V ne posodablja in se posledično zlonamerne naprave s tega seznama ne odstranjujejo. Kot rešitev te težave bi certifikat TE lahko vseboval tudi seznam V, ki jih TE lahko zastopa v procesu vzpostavitve ključa, ali pa se na Z hrani seznam vseh TE, ki zastopajo vsako V.

V protokolu vsak TE_i, ki želi sodelovati pri vzpostavitvi ključa, potrdi svoje sodelovanje, ne da bi bila ta naprava prej overjena s strani Z ali dokazala vozlišču V, da je tega sploh zmožna. Edina potrditev, ki jo V prejme o overitvi TE_i, pride v obliki zahteve po zgoščenih vrednostih določenih TE_i (sporočilo G). Ker sporočilo z zahtevo in odgovor na zahtevo nista varovana, lahko napadalec prosto doda ali odvzame naprave s prejetega ali odgovorjenega seznama vrednosti (sporočili G in H). To napadalcu ne omogoča razkritja skrivnosti, vendar lahko na takšen način povzroči neuspešno vzpostavitev ključa, kar lahko vodi tudi v napad za zavrnitev storitve. Končni napravi brez dodatne komunikacije, ki ni del protokola, ne bi ugotovili razloga za neuspešno vzpostavitev ključa.

Na začetku protokola se V in Z uskladita glede varnostne politike, vendar ta ni nikoli posredovana TE. To lahko privede do nekompatibilnosti med zgoščenimi vrednosti, ki jih V in TE dostavijo Z v sporočilih H in J. Strežnik Z bi zato moral o izbrani varnostni politiki obvestiti tudi vse TE_i v komunikaciji.

Sporočilo G vključuje enkratno vrednost, ki je bila predhodno že poslana v čistopisu (sporočilo A). Na podlagi tega lahko napadalec ustvari novo veljavno sporočilo G in ga posreduje V, preden to sporočilo pošlje Z. Ker gre za veljavno sporočilo, bi V nanj odgovorilo in zatem ne bi več odgovorilo na zahtevo, ki bi dejansko prišla od Z. V alternativnem načinu delovanja V

odgovarja na vsa veljavna sporočila, kar lahko napadalec tudi izkoristi za izvedbo napada za zavrnitev storitve. Namerno ustvarjanje velikega števila sporočil G bi prisililo V v generiranje številnih odgovorov – sporočilo H, ki pa je zagotovo najzahtevnejše sporočilo v protokolu za izgradnjo in pošiljanje. Podobno je tudi sporočilo H varovano z enkratno vrednostjo, vendar ta vrednost ni zaščitena ali povezana s preostankom sporočila, zato jo napadalec lahko preprosto odstrani in nadomesti z drugo vrednostjo, ki jo tako kot prej lahko pridobi s prisluškovanjem komunikaciji. Zgoščene vrednosti, ki se pošiljajo v sporočilu H, tudi niso zaščitene pred spremembami. V prestreženem sporočilu bi napadalec lahko prosto dodal ali odstranil vsebovane vrednosti, ne da bi prejemnik zaznal, da je med prenosom prišlo do spremembe v sporočilu.

Protokol Abdmeziem-Tandjaoui je torej zaradi svoje strukture delovanja občutljiv na napad kompromitiranega vozlišča in napad zarote. Te pomanjkljivosti bodo naslovljene v analizi protokola I. Poleg teh pomanjkljivosti so na protokol Abdmeziem-Tandjaoui možni tudi napad ponavljanja, napad za zavrnitev storitve in napad poosebljanja. Protokol tudi ne zagotavlja celovitosti v nekaterih pomembnih sporočilih vzpostavitve ključa. V protokolu I bodo odpravljene ranljivosti na naštete napade in dodano bo zagotovljene celovitost, kjer to manjka.

6.2 Izboljšani protokol za overjanje in vzpostavitev ključa v telesnih senzorskih omrežjih

Inicializacija protokola I je enaka kot v protokolu Abdmeziem-Tandjaoui. Na vozlišča V se preko varnega kanala predporazdelijo seznami tretjih entitet TE, skupaj s simetričnim ključem K_{V,TE_i} za vsako od TE. Protokol je še vedno razdeljen na pet faz, vendar se zaporedje sporočil in to, v katero fazo posamezno sporočilo spada, nekoliko spremeni. Delovanje novega protokola I je prikazano na sliki po predstavitvi posameznih faz (Slika 6.2). Ob desnem robu slike so označbe posameznih sporočil (A–K) in ob levem robu označbe, v katero fazo sporočila spadajo (faza 1–5).

Faza 1 se začne s pozdravnim sporočilom, ki ga V pošlje Z. Sporočilo vključuje predloge varnostne politike (VP), preko katere se deležniki v komunikaciji dogovorijo o uporabljenih algoritmih. Z odgovori z lastnim pozdravnim sporočilom, ki vključuje izbrano varnostno politiko in zgoščeno vrednost nove, še nikoli uporabljene enkratne vrednosti $h(N_Z)$. Zgoščena vrednost je lahko skrajšana, tako da je enake dolžine, kot bi sicer bila enkratna vrednost.

Faza 2 se začne s prošnjo V posameznim TE_i za sodelovanje pri vzpostavitvi ključa. Sporočilo poleg prejete vrednosti $h(N_Z)$ vsebuje še identiteto Z. Obe vrednosti sta šifrirani s predporazdeljenim trajnim ključem K_{V,TE_i}. Prošnja se pošlje vsem TE na seznamu, nameščenem na V. Vsaka TE_i se odloči, če bo sodelovala pri vzpostavitvi ključa. Za sodelovanje se odloči m TE od skupno n poslanih prošenj, tako da je $m \leq n$. TE_i, ki se odloči za sodelovanje, pošlje strežniku Z zahtevo po certifikatu ($CertRequest$), skupaj z lastnim certifikatom, novo ustvarjeno enkratno vrednostjo $N_{TE_i,Z}$ in od V prejeto zgoščeno enkratno vrednostjo. Po

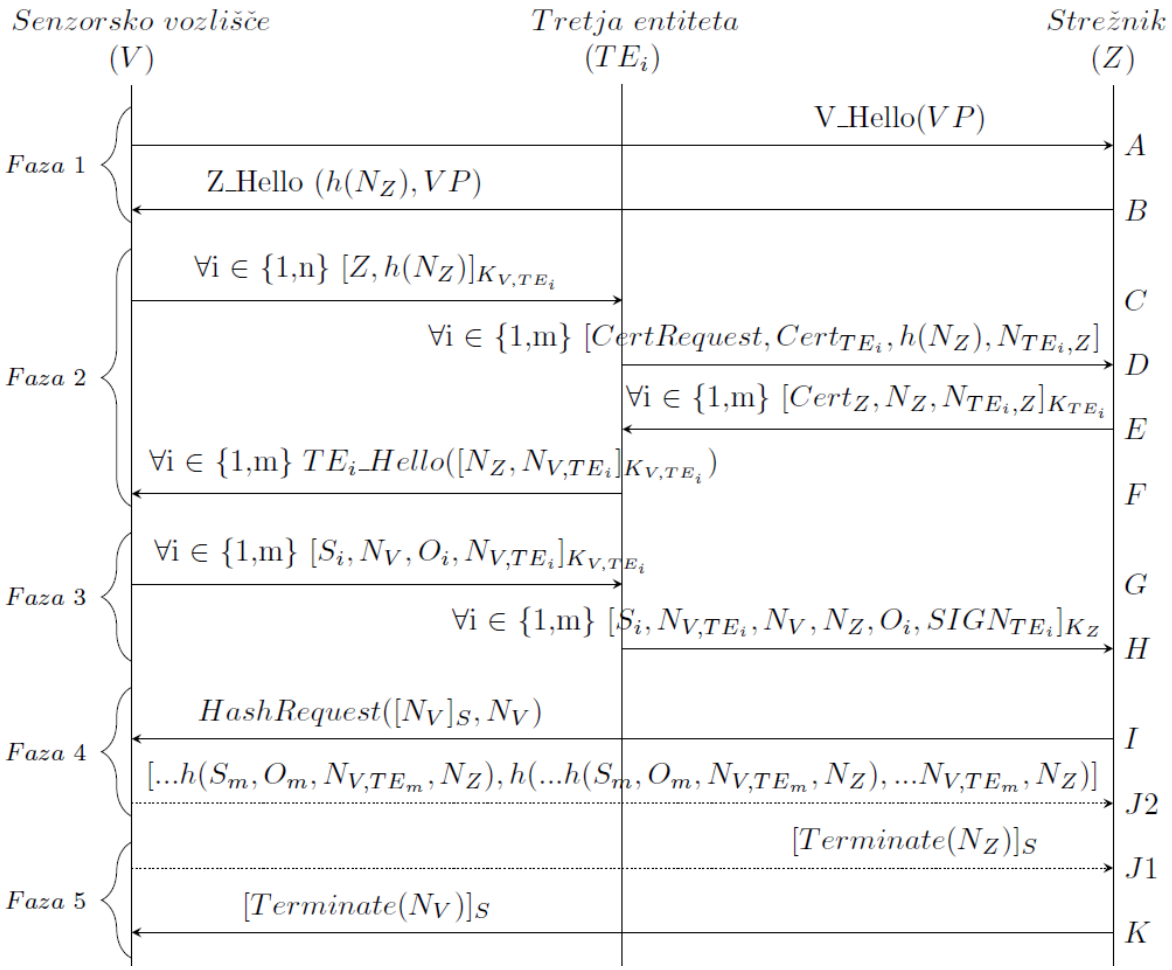
prejetju sporočila D Z overi TE_i. Če je verifikacija uspešna, Z ustvari sporočilo E in ga pošlje nazaj TE_i. Sporočilo vsebuje certifikat, prejeto enkratno vrednost in prvotno enkratno vrednost N_Z, ki jo je Z ustvaril, ko je V sprožila postopek vzpostavitve ključa, le da tokrat vrednost ni zgoščena. Celotno sporočilo je šifrirano z javnim ključem TE_i. Šele potem, ko TE_i prestane overjanje s strani Z, lahko TE_i potrdi svoje sodelovanje v vzpostavitvi ključa s pozdravnim sporočilom F. Vsak TE_i v sporočilo vključi lastno enkratno vrednost in N_Z, ki ga je dobil od Z. Sporočilo je šifrirano s K_{V,TE_i}. Tu, za razliko od originalnega protokola, TE_i ustvari ločene enkratne vrednosti za V in Z. Po prejetju in dešifriranju sporočila lahko V preveri, če je Z uspešno overil TE_i, tako da pogleda, ali je zgoščena vrednost prejetega N_Z enaka $h(N_Z)$ vrednosti, ki jo je V prejel v sporočilu B.

V novem protokolu se vrstni red faz 3 in 4 obrne, tako da faza 3 iz protokola Abdmeziem-Tandjaoui postane faza 4 in obratno.. V ustvari skrivnost S in jo razdeli na m delov (od S_1 do S_m). Sporočilo za vsako TE_i poleg S_i vključuje še N_V, O_i in N_{V,TE_i}. Parameter O_i nosi informacijo o položaju danega S_i znotraj S. Tako kot vsa sporočila med V in TE_i je tudi sporočilo G šifrirano s K_{V,TE_i}. Vsak TE_i prejeto sporočilo dešifrira in iz prejetih vrednosti ustvari novo sporočilo skupaj z dodano vrednostjo N_Z in digitalnim podpisom vseh vključenih vrednosti. Celotno sporočilo je šifrirano z javnim ključem K_Z, ki ga je TE_i prejel v sporočilu E. Po prejemu sporočila H Z tako kot vedno najprej preveri lastno enkratno vrednost (N_Z). Ko so zbrana sporočila vseh TE, Z preveri, da vsa vsebujejo enak N_V. TE_i, ki je poslalo različno vrednost N_V, ne zastopa V in ni prejela vrednosti od vozlišča. Takšno entiteto je treba izločiti. Iz prejetih podatkov Z ustvari celotno skrivnost S.

Faza 4 se začne na strežniku Z, ki pošlje sporočilo I. Sporočilo vsebuje z novo pridobljeno skrivnostjo S šifrirano vrednost N_V, preko katere Z dokaže poznavanje skrivnosti vozlišču. V protokolu Abdmeziem-Tandjaoui zaradi drugačne strukture protokola Z v tej točki še ni poznal S. Če lahko V dešifrira prejeto vrednost (t. i. potrjevanje ključa), je bila vzpostavitev ključa uspešna in lahko V pošlje končno sporočilo J1, s katerim se protokol I zaključi. V nasprotnem primeru je v komunikaciji prišlo do napake ali pa se je vanjo vključila zlonamerna entiteta. Vedno se pošlje samo eno od sporočil J1 ali J2. Sporočilo vsebuje vse potrebne informacije $(h(S_i, O_i, N_{V,TE_i}, N_Z))$, na podlagi katerih lahko Z preveri, da so podatki, ki so mu jih posredovale posamezne TE_i, resnični. Zadnja vrednost v sporočilu je zgoščena vrednost vseh predhodnih vrednosti sporočila, enkratnih vrednosti N_{V,TE_i}, ki si jih V deli z vsemi TE in enkratne vrednosti N_Z. Na podlagi prejetih informacij lahko Z izloči zlonamerne TE, ki v prihodnosti ne bodo več mogle sodelovati pri vzpostavitvi ključa.

Faza 5 je zadnja faza, ki se lahko zaključi v dveh točkah. Prva (J1) je bila omenjena v prejšnji točki. Potem ko Z zgradi posredovano skrivnost S iz prejetih S_i, pokaže svoje poznavanje te skrivnosti v sporočilu I. V primeru, da se ni noben del skrivnosti izgubil v prenosu oziroma so vse TE korektno posredovale pravilne podatke, bo bilo V sposobno dešifrirati poslano vrednost $[N_V]_S$ in zaključiti vzpostavitev ključa s sporočilom J1. V nasprotnem primeru mora V posredovati Z seznam vrednosti, ki predstavljajo vse TE, ki jo zastopajo. V tem primeru

vzpostavitev ključa zaključi Z, s sporočilom K, šifriranim s skrivnostjo S, ki jo je prilagodil na podlagi vsebine sporočila J2.



Slika 6.2: Izmenjava sporočil v novem protokolu I [205].

6.2.1 Izboljšave novega protokola I

V tem poglavju bomo izpostavili razlike med protokolom Abdmeziem-Tandjaoui in protokolom I ter razložili, zakaj smo te razlike uvedli v protokol I.

Iz prvega sporočila je bila odstranjena vrednost N_V. Ta vrednost bo posredovana Z pozneje preko TE v šifrirani obliki. Sporočilo B ostane v osnovi enako, vendar se enkratna vrednost posreduje v obliki izvlečka zgoščevalne funkcije. Dejanska enkratna vrednost bo posredovana kasneje preko varnega kanala in z namenom potrditve stika med TE_i in Z. V fazi 2 je odgovor TE_i na prošnjo o sodelovanju s strani V preložen na konec faze, ko TE_i prejme parametre s strani Z. Zato da lahko sprejme ponudbo o sodelovanju, mora namreč sedaj TE_i prejeti N_Z, ki ni javno znan in ni bil nikoli poslan preko javnega kanala, vendar ga V lahko preveri, ker ima izvleček iste vrednosti ($h(N_Z)$) iz sporočila B. Enkratne vrednosti, ki jih ustvari TE_i, so v novem protokolu I različne glede na to, ali je ta vrednost najprej poslana V ali Z. Za enkratno vrednost,

ki je poslana vozlišču V, je pomembno, da je naključna, saj bo kasneje uporabljena za zagotavljanje celovitosti, in uporaba časovnih žigov ali števca bi v veliki meri povečala verjetnost odkritja teh vrednosti.

Kot smo omenili, se je vrstni red 3. in 4. faze iz originalnega protokola v protokolu I obrnil. V novem protokolu V posreduje S_i preko TE_i, preden pridobi od Z zahtevo po seznamu vpletenih TE. To omogoča preprostejši prenos S, saj se na takšen način lahko največjemu sporočilu in najzahtevnejšemu sporočilu, ki ga mora V ustvariti in poslati, v celoti izognemo. V fazi 3 je bil dodan popolnoma nov parameter O_i, ki je pokazatelj vrstnega reda S_i, na podlagi katerega zgradi S. Vrednosti tega parametra ne smejo biti zaporedne, ampak naključne (vendar še vedno v pravem vrstnem redu) znotraj možnih vrednosti parametra, tako da tudi več sodelujočih TE_i ni sposobno določiti, ali imajo zaporedne dele skrivnosti.

V primerjavi s protokolom Abdmeziem-Tandjaoui se v novem protokolu I enkratna vrednost N_V prenese do Z veliko pozneje v procesu in preko vsakega TE. Na takšen način lahko zagotovimo, da se vrednost preda samo TE_i, ki so bile uspešno overjene s strani Z. Vrednost N_V služi kot povratni dokaz strežniku, da so vse TE_i, ki so v komunikaciji z njim, tudi v komunikaciji z V. Zato se ta vrednost tudi nikoli ne posreduje v čistopisu (sicer bi jo drugi TE pridobili s prisluškovanjem), dokler vsi TE_i ne pokažejo svojega poznavanja vrednosti (N_V se nevarovana pošlje v sporočilu I). Istočasno to tudi zagotavlja, da nihče (razen potencialno TE_i, ki sodelujejo v vzpostavitvi ključa) ne more ponarediti sporočila I (ker N_V ni javno znan). To je pomembno, ker bi sicer bilo V primorano vračati sporočila J2 za lažne zahteve in sporočilo J2 je največji porabnik virov senzorskega vozlišča v celem protokolu. Sporočilo J2 je veliko bolj zahtevno kot primerljivo sporočilo H iz originalnega protokola, vendar je opcijsko, saj se pošlje le, ko je na komunikacijo vplivala zlonamerna entiteta. Takšen način delovanja zviša raven varnosti protokola za ceno majhnega povišanja izrabe virov. Sestava sporočila J2 zagotavlja celovitost sporočila (sporočila ni mogoče spremeniti, ne da bi naslovnik to opazil) in vrednosti v sporočilu so različne ob vsaki vzpostavitvi ključa. Nobena od teh dveh lastnosti ni veljala v protokolu Abdmeziem-Tandjaoui. Vključitev vseh vrednosti N_{V,TE_i} zagotavlja, da niti same TE ne morejo neopazno spremeniti sporočila (razen če bi v napadu sodelovale popolnoma vse TE, v takem primeru pa je napad vedno uspešen, ker vse TE tako ali tako vedo celoten S). Na podlagi sporočila J2 lahko strežnik odkrije katere tretje entitete so posredovale nepravilne vrednosti S_i.

6.3 Varnostna analiza protokola I

V tem poglavju predstavimo in primerjamo varnostne lastnosti izboljšanega protokola I z varnostnimi lastnostmi protokola Abdmeziem-Tandjaoui. Uporabljen je hevristični model analize. Varnostno analizo oblikujemo po vzoru varnostne analize, ki je bila opravljena za protokol Abdmeziem-Tandjaoui [122], in vključimo relevantne varnostne lastnosti ter odpornosti na napade, predstavljene v poglavjih 4.1 in 4.2. Novi protokol I je v osnovi zelo podoben originalnemu protokolu, ker uporablja enak mehanizem za vzpostavitev ključa.

Posledično so tudi varnostne lastnosti izboljšanega protokola podedovane od protokola Abdmeziem-Tandjaoui. Protokol I ohrani ali izboljša zaupnost, razširljivost, celovitost podatkov, overjanje entitet in odpornost na napade. Faza inicializacije je identična v obeh protokolih in predporazdeljene vrednosti so tudi enake. Izboljšani protokol I ohranja tudi nabor uporabljenih osnovnih kriptografskih elementov.

Vse skrivne vrednosti so v protokolu I prenesene preko šifrirane komunikacije. V primeru simetričnega šifriranja se uporabijo predporazdeljeni ključi, medtem ko je drugi del komunikacije varovan z asimetrično kriptografijo ob podpori infrastrukture javnih ključev. V primerjavi z originalnim protokolom je veliko večji delež komunikacije šifriran. To zagotavlja boljšo zaupnost, vendar je tudi računsko zahtevnejše, o čemer bomo govorili v nadaljevanju. Z vsako izvedbo protokola se sejni ključ spremeni na nedeterminističen način, kar okrepi zaupnost in preprečuje dolgoročne napade. Z uporabo kod za overitev sporočila in digitalnih podpisov protokol zagotavlja overjanje pošiljateljev. Poleg overjanja naprav v neposredni komunikaciji novi protokol omogoča tudi preverjanje, ali so se TE_i uspešno overile obema končnima napravama (V in Z). Potrebno je zagotoviti tudi celovitost podatkov. Ta ni bila zagotovljena v sporočilu H protokola Abdmeziem-Tandjaoui. Prilagojeno sporočilo J2 v izboljšanem protokolu I preprečuje spreminjanje vsebine sporočila, kar je zelo pomembno, ker sporočilo nosi pomembne informacije o deležnikih pri vzpostavitvi ključa, na podlagi katerih lahko Z odkrije zlonamerne naprave v komunikaciji. Sporočilo G v originalnem protokolu bi lahko poslala katera koli naprava, ne da bi V to opazilo. V novem protokolu ima isto funkcijo sporočilo I, ki je dodatno zaščiteno, tako da vsebina sporočila ni vnaprej znana entitetam, ki niso vključene v komunikacijo (tudi prisluškovalcem ni znana).

Kot smo že omenjali, so protokoli s takšno strukturo, kot sta originalni in izboljšani protokol I, dovzetni na obliko **napada poosebljanja**, ker si dve ali več TE lahko izmenjujejo podatke, ki jih prejemajo (poosebljajo ena drugo), in se tako uspešno overijo pri V in Z, čeprav se z vsako napravo overi druga TE. Napadalec bi takšno ranljivost lahko izkoristil za povečanja vpliva v omrežju s pomočjo TE, nad katerimi je prevzel nadzor. Te naprave bi tudi lahko izgubile veljavnost certifikatov, vendar to ne bi vplivalo na napad, dokler ima napadalec pod kontrolo eno samo TE, ki se lahko uspešno overi pri Z. Za preprečevanje takšnega napada je potrebno Z seznaniti s tem, katero V lahko zastopajo kateri TE. Ta podatek bi se lahko vključil v sam certifikat TE ali pa bi Z moral hraniti enake sezname, kot so predporazdeljeni na V. S podatkom o veljavnih zastopnikih lahko Z komunikacijo z vsemi TE, ki nimajo pravice zastopanja določenega V, preprosto zavrže.

Oblika protokola, ki se za svoje delovanje zanaša na TE, sprejme določeno tveganje **kompromitiranja** teh **naprav**. Z ni problematičen, saj se nahaja v strogo varovanem okolju. Vozlišča V so bolj dovzetna za odtujitev naprave, toda nahajajo se na telesu uporabnika, kjer je neopazna odtujitev in potem ponovna vrnitev naprave na telo brez vedenja uporabnika praktično nemogoča. TE so bolj dovzetne za takšen napad, saj je njihovo varovanje v celoti odvisno od njihovih lastnikov, ki pa lahko teh naprav ne ščitijo ustrezno.

Sporočilo G v originalnem protokolu je glede na delovanje protokola (v predstavitvi protokola ni navedeno natančno, kako ta del protokola deluje) omogočalo napadalcu prekinitev vzpostavitve ključa ali pa **napada za zavrnitev storitve**. Sporočilo namreč ni na noben način zaščiteno. Posledično ga lahko pošlje vsakdo, ki je prisluškoval vzpostavitvi ključa in je prestregel vrednost N_V. Ob prejetju takšnega sporočila lahko V reagira na dva načina. Prvi je, da po prejetem sporočilu ne sprejme drugih zahtev z enako enkratno vrednostjo. Če v tem primeru napadalec pošlje takšno sporočilo pred Z, potem vzpostavitev ne bo nikoli dokončana, saj V ne bo sprejelo legitimne zahteve od Z. Alternativno lahko V sprejme vsa sporočila in nanje ustvari odgovore (sporočilo H). Takšno delovanje lahko napadalec izkoristi in napravi pošlje veliko število zahtev ter s tem povzroči napad za zavrnitev storitve ali pa vsaj izčrpa rezerve električne energije na V. Protokol I (sporočilo I) reši ta problem, tako da se enkratna vrednost N_V predhodno nikoli ne pošlje preko javnega kanala nešifrirana. Zahteva z ustrezno enkratno vrednostjo lahko zato pride le od Z in V lahko vse ostale zahteve zavrže.

Napad s ponavljanjem je zelo preprost napad, pred katerim se oba protokola varujeta z uporabo enkratnih vrednosti. Vendar je uporaba enkratnih vrednosti v sporočilu H originalnega protokola neprimerna, saj vrednosti niso zaščitene oziroma so enake ob vsakem izvajanju protokola, zato jih napadalec lahko shrani in veljavno uporabi v prihodnosti. Uporabljena enkratna vrednost ne varuje pred tem, ker ni povezana s preostalimi podatki v sporočilu in jo lahko zato napadalec prosto spreminja. Novi protokol te pomanjkljivosti odstrani. Posamezne vrednosti v sporočilu se spreminjajo ob vsaki vzpostavitvi novega ključa in celotno sporočilo je zaščiteno na način, da ga ni mogoče neopazno spremeniti. Celovitost sporočila je zagotovljena s pomočjo zgoščene vrednosti, ki vsebuje celotno vrednost preostalega dela sporočila in dodatne vrednosti, ki jih vse pozna samo Z (od N_{V,TE_1} do N_{V,TE_m}).
Napad vrinjenega napadalca v protokolu I ni mogoč, ker se vsi skrivni podatki prenašajo v šifrirani obliki. Posrednik se ne more v komunikaciji z V pretvarjati kot legitimna entiteta, dokler je predporazdeljen simetrični ključ skriven (če se ta razkrije, varna vzpostavitev ključa ni več mogoča), medtem ko med TE_i in Z napad vrinjenega napadalca ni mogoč zaradi uporabe infrastrukture javnih ključev.

Napad Sybil bi v protokolu I izkoriščal večje število TE tako, da bi se v omrežju ustvarile fiktivne TE, ki bi predstavljale večji del vseh TE in posledično razkrile velik del S. V novem ali originalnem protokolu to ni mogoče, ker se vse TE overijo in posledično ni mogoče vnašanje lažnih entitet v sistem.

Težava v originalnem protokolu je tudi možnost TE_i, da sprejme potrdilo o sodelovanju pri vzpostavitvi ključa brez kasnejšega dejanskega sodelovanja pri vzpostavitvi in z namenom hitrejše porabe virov V. Da bi takšno početje preprečil, protokol I vsebuje izmenjavo vrednosti ($N_Z\ in\ N_V$) med V in Z, s katero se lahko vsaka končna naprava prepriča, da vsak TE_i dejansko komunicira tudi z drugo končno napravo. Vendar ker je za to, da opazimo odstopanje ene TE_i od drugih, potrebno uporabiti isto vrednost za vse TE_i, to pomeni, da lahko TE_i obide to varovanje s sodelovanjem s TE, ki dejansko sodeluje v vzpostavitvi ključa. Novi protokol torej zmanjša verjetnost takšnega napada, vendar je ne izniči popolnoma.

Napad zarote je zadnji pomemben napad, ki je zelo relevanten za protokole, ki vsebujejo porazdeljen prenos skrivnosti. V takšnem napadu TE sodelujejo z namenom razkritja S. V primeru, da sodelujejo vse TE, ki so sprejele prošnjo za sodelovanje pri vzpostavitvi ključa, je skrivnost takoj razkrita, saj vse TE skupaj vsebujejo vse podatke, ki si jih izmenjata V in Z. Vendar je že nekaj sodelujočih TE dovolj za znižanje varnosti na neželeno raven. Priporočila Narodnega urada za standarde in tehnologijo Združenih držav Amerike (angl. National Institute of Standards and Technology – NIST) [208] postavljajo minimalno dolžino varnega ključa za uporabo s simetričnimi šiframi na 112 bitov. Zato bi ob uporabi protokola I ali protokola Abdmeziem-Tandjaoui priporočili uporabo vsaj osmih TE. V takšnem primeru bi vsaka TE_i poznala natančno eno osmino (16 bitov) celotne S, ki je dolga 128 bitov. To pomeni, da bi količina neznanih bitov znašala natančno 112. Istočasno to tudi pomeni, da bi vsaka oblika zarote oziroma sodelovanja med TE znižala raven varnosti pod minimalno priporočilo, kar bi izrazito povečalo verjetnost uspešnega ugibanja skrivnosti. Da bi to preprečili, je potrebno veliko število TE ali večja dolžina S. Obstaja tudi možnost skrivnosti takšne velikosti, da bi posamezen del S_i bil velik 128 bitov (združeni S_i bi se na V in Z lahko ponovno skrčili na primernejšo velikost s pomočjo zgoščevalne funkcije), kar bi zagotavljalo, da bi ob sodelovanju vseh razen ene same TE varnost končne S še vedno bila odvisna od 128 bitov skrivnih podatkov (kar je ob času pisanja disertacije priporočena vrednost).

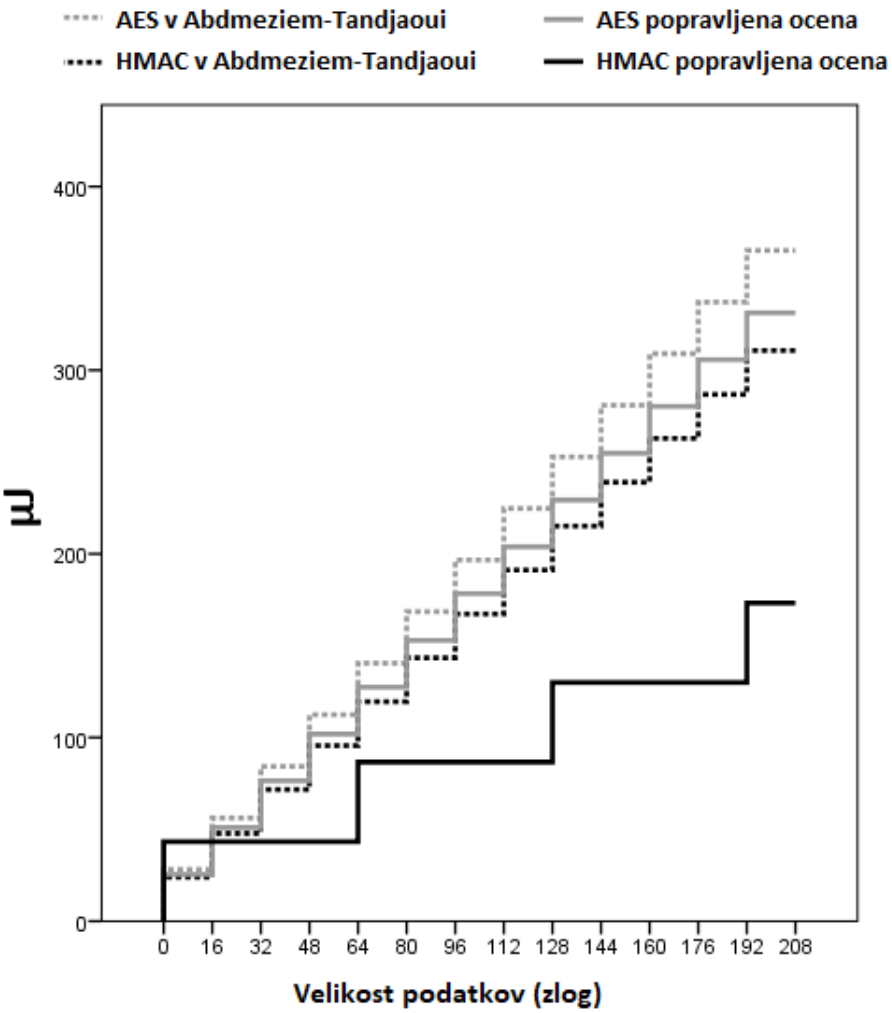
6.4 Analiza učinkovitosti protokola I

Poglavje je namenjeno analizi učinkovitosti novega protokola I. Protokol I je izboljšava obstoječega protokola Abdmeziem-Tandjaoui [122], ki deluje na novi ideji prenosa zahtevnih operacij s strojno omejenih naprav na tretje naprave, ki nimajo takšnih omejitev. Glede na naš pregled literature je to edini predlagani protokol za vzpostavitev ključa v TSO, ki deluje na takšen način, zato je tudi analiza učinkovitosti temu prilagojena. Analiza se osredotoča na primerjavo učinkovitosti novega protokola I z originalnim protokolom in upošteva samo zahtevnost delovanja senzorskega vozlišča V, ker je to edina naprava v komunikaciji protokola, ki ima omejene strojne vire in zaloge energije. Poglavje se začne s pregledom analize protokola Abdmeziem-Tandjaoui, v kateri zasledimo nekaj nedoslednosti pri uporabi izbranih algoritmov in vrednotenju porabe energije glede na rezultate predhodnih raziskav. Za analizo učinkovitosti protokol I uporabimo pristope, ki so se ob pregledu uporabljenih metod preverjanja učinkovitosti protokolov vzpostavitve ključa za uporabo v TSO (poglavje 5.3), izkazali za najpogosteje uporabljene pristope v primeru tradicionalnih protokolov (preverjanje porabe pomnilnika, računske zahtevnosti, komunikacijske zahtevnosti in skupna poraba energije). Protokol I ohranja začetno stanje originalnega protokola Abdmeziem-Tandjaoui, zato se poraba pomnilnika ne spremeni. Primerjava računske in komunikacijske zahtevnosti ter ocena njune električne porabe med originalnim protokolom ter novim protokolom I je podana v zadnjem delu tega poglavja.

Analiza učinkovitosti protokola Abdmeziem-Tandjaoui je osnovana na podlagi vrednotenja porabe električne energije ob sodelovanju različnega števila TE. Za to so avtorji protokola

uporabili ocene porabe električne energije šifriranja (algoritem AES) in izdelave kode za overitev sporočila (HMAC-SHA-1 – način ustvarjanja kode za overitev sporočila z uporabo zgoščevalne funkcije SHA-1), predstavljene v raziskavi [209]. V tej raziskavi so na podlagi meritev delovanja obeh algoritmov ovrednotili porabo električne energije. V analizi protokola Abdmeziem-Tandjaoui smo zasledili nedoslednosti z ocenami, ki so bile podane v tem članku. V raziskavi [209] so meritve izvedene nad vhodnimi podatki velikosti 29 zlogov za AES in 33 zlogov za HMAC. Avtorji originalnega protokola so želeli v analizi uporabiti bolj pogosto velikost podatkov, ki je tipično večkratnik 128 bitov (16 zlogov). Zato so oceno prilagodili tako, da so vrednost pomnožili z $\frac{16}{29}$ za oceno porabe AES in $\frac{16}{33}$ za oceno HMAC in na tak način pridobili sorazmeren delež porabljene energije med velikostjo vhodnih podatkov v meritvah raziskave [209] in velikostjo podatkov, glede na katero so želeli dane vrednosti prilagoditi (16 zlogov). Pri tem so pozabili upoštevati, da tako AES kot tudi SHA-1 (HMAC prevzame lastnosti algoritma, ki je uporabljen) obdelujejo podatke v blokih. Ne glede na količino podatkov v bloku se preostanek bloka vedno bitno zapolni (angl. padding) in strošek obdelave istega števila blokov je vedno enak. V primeru šifriranja 16 zlogov podatkov z algoritmom AES, ki uporablja bloke velikosti 128 bitov, je zahtevnost za polovico manjša od šifriranja 29 zlogov (čeprav podatki v tem primeru ne zapolnijo v celoti drugega bloka). Odstopanje med uporabljeno oceno porabe energije v analizi protokola Abdmeziem-Tandjaoui in oceno, podano v [209], je še veliko večje ob uporabi HMAC-SHA-1. SHA-1 namreč uporablja za svoje delovanje blok velikosti 512 bitov (64 zlogov), kar pomeni, da je električna poraba enaka za obdelavo podatkov velikosti 16 ali 33 zlogov. Poraba bi ostala enaka do podatkov velikosti 64 zlogov, kjer bi bil prvi blok v celoti zapolnjen. Pri tem je treba upoštevati delovanje zgoščevalne funkcije SHA-1, kjer vhodnim podatkom vedno sledi bit, nastavljen na vrednost 1. Dodatno se v zadnjih 8 zlogov bloka (če ni dovolj prostora, se doda nov blok) vpiše dolžina vhodnih podatkov. To pomeni, da je največja možna dolžina vhodnih podatkov, tako da se vsi obdelajo v enem bloku, 447 bitov. Ker so podatki tipično podani v zlogih, se ta velikost dodatno zmanjša na 440 bitov (55 zlogov).

Na naslednjem grafu (Slika 6.3) je prikazano odstopanje med oceno porabe električne energije algoritmov AES in HMAC-SHA-1, kot so jo uporabili avtorji protokola Abdmeziem-Tandjaoui, in oceno, ki bi bila pravilno pridobljena iz raziskave [209]. Sive črte predstavljajo porabo šifrirnega algoritma AES, črne črte predstavljajo HMAC-SHA-1, prekinjene črte so ocene porabe, vzete iz analize protokola Abdmeziem-Tandjaoui, in polne črte so prilagojene ocene porabe električne energije glede na dejansko delovanje obeh algoritmov. Velikost podatkov HMAC-SHA-1 že vključuje režijske stroške (angl. overhead). Iz grafa je razvidno, da so ocene porabe energije v analizi protokola Abdmeziem-Tandjaoui nekoliko višje v primeru šifre AES in veliko višje v primeru HMAC-SHA-1 v primerjavi z ocenami porabe, ki pri izračunu ocene pravilno upoštevajo delovanje vrednotenih algoritmov. Ocene algoritma HMAC-SHA-1 v analizi protokola Abdmeziem-Tandjaoui so toliko višje predvsem zaradi zmotnega razmišljanja o obdelavi podatkov v veliko manjših blokih, kot se dejansko obdelujejo. Nove ocene porabe električne energije tudi sovpadajo s splošno sprejetim dejstvom, da so zgoščevalne funkcije manj računsko zahtevne, kot je simetrično šifriranje [210].



Slika 6.3: Odstopanje v oceni porabe električne energije v raziskavi Abdmeziem-Tandjaoui in popravljeni oceni porabe [205].

Ker na podlagi članka, v katerem je bil originalni protokol predstavljen, ni mogoče razbrati, na kakšen način so bile končne številke porabe električne energije protokola izdelane (katere ocene porabe so bile uporabljene za izračun porabe zgoščevalnih funkcij in kakšne velikosti so bili posamezni parametri), in ker tiste ocene porabe, za katere vemo, da so bile uporabljene, niso bile pravilne, neposredna primerjava z rezultati analize protokola Abdmeziem-Tandjaoui ni mogoča. Zato smo ustvarili primerjavo na podlagi računskih operacij in velikosti podatkov v komunikaciji vozlišča V. To je najbolj nevtralen način primerjave, ki ni odvisen od strojne opreme, kakovosti implementacije ali uporabljenih algoritmov. Primerjavo smo ustvarili tudi na podlagi ocen porabe energije v računskih operacijah in količini komunikacije. Ker iz analize protokola Abdmeziem-Tandjaoui ni mogoče pridobiti vseh podatkov, bomo uporabili lastne velikosti posameznih parametrov, ki so uporabljeni v protokolih. Nekatere od teh vrednosti so morda večje, kot je trenutno potrebno ali praktično za uporabo, vendar to ne vpliva na primerjavo, kjer se za oba protokola uporabljajo enake vrednosti. Analiza računske zahtevnosti in učinkovitosti obeh protokolov izključuje vrednosti *Hello* in *Terminate* sporočil ter

vrednosti varnostne politike VP. Te se med obema protokoloma uporabljajo identično, zato zaradi tega v primerjavi ne nastanejo razlike. Analiza učinkovitosti je omejena na vrednotenje računske zahtevnosti in učinkovitosti komunikacije, ker sta si sicer protokola toliko podobna, da so metrike, kot je poraba pomnilnika ali stroški poslušanja na kanalu, enake za oba protokola. Analiza učinkovitosti vključuje samo senzorsko vozlišče V, ker je to edina naprava v protokolu, ki ima omejene strojne vire in vir energije. Notacija, uporabljena v analizi učinkovitosti, in oznake parametrov ter njihove velikosti so zapisane v spodnji tabeli (Tabela 6.2).

Tabela 6.2: Definicija simbolov, uporabljenih v analizi učinkovitosti.

Simbol	**Opis**
$h()$	Kriptografska zgoščevalna funkcija (SHA-1)
$E()$ in $D()$	Operacija šifriranja in dešifriranja (AES) ter istočasno velikost izhodnih podatkov operacije (od vhodnih podatkov odvisen večkratnik 128 bitov)
N	Velikost enkratne vrednosti (128 bitov)
H	Velikost zgoščene vrednosti (160 bitov)
$\overline{H}$	Zgoščena vrednost, skrajšana na velikost enkratne vrednosti (128 bitov)
Z	Velikost identitete strežnika Z (128 bitov)
n	Število TE, ki jih V hrani v pomnilniku
m	Število TE, ki sodelujejo v vzpostavitvi ključa (minimalno 2)
S_i	Del skrivnosti S (glede na število m sorazmerni delež velikosti S – $\frac{128\ bitov}{m}$)
O	Velikost parametra O_i (≤ 64 bitov, odvisno od števila m)
K	Velikost predporazdeljenih ključev med V in TE (128 bitov)

V naslednji tabeli (Tabela 6.3) je seznam vseh računskih operacij in lokacij, kje v protokolu se izvedejo (v katerem sporočilu). Iz hitrega pregleda računskih operacij v vsakem protokolu je takoj jasno, da je novi protokol I računsko zahtevnejši od originalnega protokola. Razlika je predvsem posledica dodatnega šifriranja sporočil med V in TE_i, ki preprečuje prisluškovalcem, da bi pridobili vrednosti, ki se izmenjajo med delovanjem protokola in s pomočjo katerih bi lahko ogrozili uspešnost vzpostavitve ključa.

Tabela 6.3: Seznam računskih operacij, ki jih opravi senzorsko vozlišče v protokolu Abdmeziem-Tandjaoui in novem protokolu I.

Protokol Abdmeziem-Tandjaoui		**Protokol I**	
Sporočilo	**Računska zahtevnost**	**Sporočilo**	**Računska zahtevnost**
C	$n \times E(3N)$	C	$n \times E(N + \bar{H})$
H	$m \times h(K)$	F	$m \times D(2N) + h(N)$
I	$m \times E(N + S_i)$	G	$m \times E(3N)$
K	$D(N)$	I	$D(N)$
		J1	$E(N)$
		J2	$m \times h(2N + S_i + O) +$ $h(m \times H + (m + 1) \times N)$
		K	$D(N)$

Glede na ta seznam računskih operacij in ocen porabe električne energije vsake operacije smo ustvarili oceno porabe električne energije izvajanja obeh protokolov. Ocene porabe za algoritma AES in SHA-1 so bile pridobljene iz [209]. Strošek šifriranja AES enega bloka (128 bitov) je ocenjen na 25,48 nJ, medtem ko je zgoščevanje enega bloka SHA-1 (512 bitov) ocenjeno na 43,32 nJ. Operaciji šifriranja in dešifriranja štejemo kot enako zahtevni. Vrednotenje porabe je opravljeno za različno število TE (m), kjer smo se omejili na situacije, ko vse vse TE_i odzovejo na prošnjo po sodelovanju pri vzpostavitvi ključa (n=m). Končna ocena porabe energije računskih operacij je predstavljena v spodnji tabeli (Tabela 6.4). Za protokol I je najprej navedena poraba energije v zahtevnejšem primeru delovanja (uporaba sporočil J2 in K), zatem pa je v oklepaju zapisana še poraba v optimalnem delovanju (uporaba sporočila J1). Kot je pričakovati iz podatkov prejšnje tabele, je računska zahtevnost protokola I večja od originalnega protokola. Ta razlika je očitna predvsem ob uporabi majhnega števila TE. Z večanjem m se sorazmerna razlika med protokoloma manjša. Ob uspešnem posredovanju S do Z, kar V preveri po sporočilu I, sporočilo J2 nikoli ne ustvari. Ker je sporočilo J2 računsko najzahtevnejše, je ob takšnem delovanju računska zahtevnost protokola I veliko manjša in bolj primerljiva s tisto pri protokolu Abdmeziem-Tandjaoui.

Tabela 6.4: Ocena porabe električne energije senzorskega vozlišča v računskih operacijah protokola Abdmeziem-Tandjaoui in novega protokola I.

Število TE (n=m)	**Poraba energije v računskih operacijah protokola Abdmeziem-Tandjaoui (nJ)**	**Poraba energije v računskih operacijah protokola I (nJ)**
2	366,9	624,3 (451)
4	708,4	1111 (807,7)
6	1049,8	1597,6 (1164,4)
8	1391,2	2084,3 (1521,2)
10	1732,7	2571 (1877,9)

Učinkovitost komunikacije na podlagi izmenjanih sporočil je predstavljena v naslednji tabeli (Tabela 6.5). Tabela vključuje informacije o tipih podatkov, ki so prisotni v vsakem sporočilu, in podatek o tem, ali so vrednosti poslane (T) ali prejete (R). Rezultati ponovno kažejo, da je protokol I zahtevnejši za delovanje kot protokol Abdmeziem-Tandjaoui. Večjo količino komunikacije gre pripisati predvsem preverjanju, da se TE overijo na obeh končnih napravah.

Tabela 6.5: Seznam poslanih in prejetih vrednosti senzorskega vozlišča v protokolu Abdmeziem-Tandjaoui in novem protokolu I.

Protokol Abdmeziem-Tandjaoui			**Protokol I**		
Sporočilo	**T/R**	**Podatki**	**Sporočilo**	**T/R**	**Podatki**
A	T	N	B	R	$\overline{H}$
B	R	N	C	T	$n \times E(Z + \overline{H})$
C	T	$n \times E(Z + 2N)$	F	R	$m \times E(2N)$
D	R	$m \times N$	G	T	$m \times E(S + O + 2N)$
G	R	N	I	R	$N + D(N)$
H	T	$m \times H + N$	J2	T	$(m + 1) \times H$
I	T	$m \times E(S_i + N)$	J1	T	$E(N)$
K	R	$D(N)$	K	R	$D(N)$

Za izračun ocene porabe električne energije komuniciranja smo sešteli količine poslanih in prejetih podatkov glede na število TE (m). Oceno porabe električne energije za pošiljanje in prejemanje podatkov smo pridobili iz raziskave [211], kjer so ocenili porabo energije za pošiljanje enega bita podatkov na 0,72 μJ in na 0,81 μJ za prejemanje enega bita podatkov. Rezultati vrednotenja porabe energije v namene komunikacije so prikazani v spodnji tabeli (Tabela 6.6). Vrednost velikosti podatkov vsebuje poslane in prejete podatke, medtem ko je porabljena energija izračunana glede na to, ali se podatki pošiljajo ali prejemajo. Ocena porabe pokaže, da se v novem protokolu I pošlje in prejme nekoliko več podatkov na vozlišču V, kot se jih je v originalnem protokolu. Posledično je tudi poraba energije večja (skoraj 15 %). Ponovno je potrebno upoštevati, da ima protokol I možnost preprostejšega delovanja, kjer se namesto sporočil J2 in K pošlje samo sporočilo J1. Vrednotenje takšnega delovanja je v tabeli prikazano v oklepaju. V primeru optimalnega delovanja je nov protokol I komunikacijsko učinkovitejši kot protokol Abdmeziem-Tandjaoui. Ker so ocene porabe energije za računske operacije in komunikacijo pridobljene iz različnih virov, te niso neposredno primerljive, vendar je vseeno očitno, da so stroški komunikacije veliko večji kot stroški računskih operacij.

Tabela 6.6: Stroški komunikacije senzorskega vozlišča v protokolu Abdmeziem-Tandjaoui in novem protokolu I.

Število TE (n=m)	Protokol Abdmeziem-Tandjaoui		Protokol I	
	Velikost podatkov (bit)	Porabljena energija (μJ)	Velikost podatkov (bit)	Porabljena energija (μJ)
2	2496	1854,7	2784 (2304)	2096,6 (1739,5)
4	4352	3214,1	4896 (4096)	3663,4 (3075,8)
6	6208	4573,4	7008 (5888)	5230,1 (4412,2)
8	8064	5932,8	9120 (7680)	6796,8 (5748,5)
10	9920	7292,2	11232 (9472)	8363,5 (7084,8)

Primerjava učinkovitosti protokola I z originalnim protokolom Abdmeziem-Tandjaoui pokaže, da dodatna varnost izboljšanega protokola, ki je bila predstavljena v prejšnjem poglavju, negativno vpliva na učinkovitost protokola. Ravnovesje med porabo virov in ravnjo varnosti je vedno kompromis pri zagotavljanju varnosti. V tem primeru, je po našem mnenju originalni protokol imel preveč varnostnih pomanjkljivosti, da bi upravičil nekoliko manj zahtevno delovanje. Poleg tega, nov protokol I uvede tudi alternativno delovanje, ki ima izrazito izboljša računsko in komunikacijsko porabo energije, tako da je celoten protokol bolj učinkovito od predhodnega protokola. Kljub temu, da se protokol I na takšen način izvede le v primerih, ko med vzpostavitvijo ključa ne pride do napak ali napada, ki bi preprečil uspešno izmenjavo ključa, je skupaj z izboljšano varnostjo, protokol I zagotovo boljša alternativa protokolu Abdmeziem-Tandjaoui.

7 Razvoj protokola za overjanje in dogovor o ključu za uporabo v brezžičnih telesnih senzorskih omrežjih

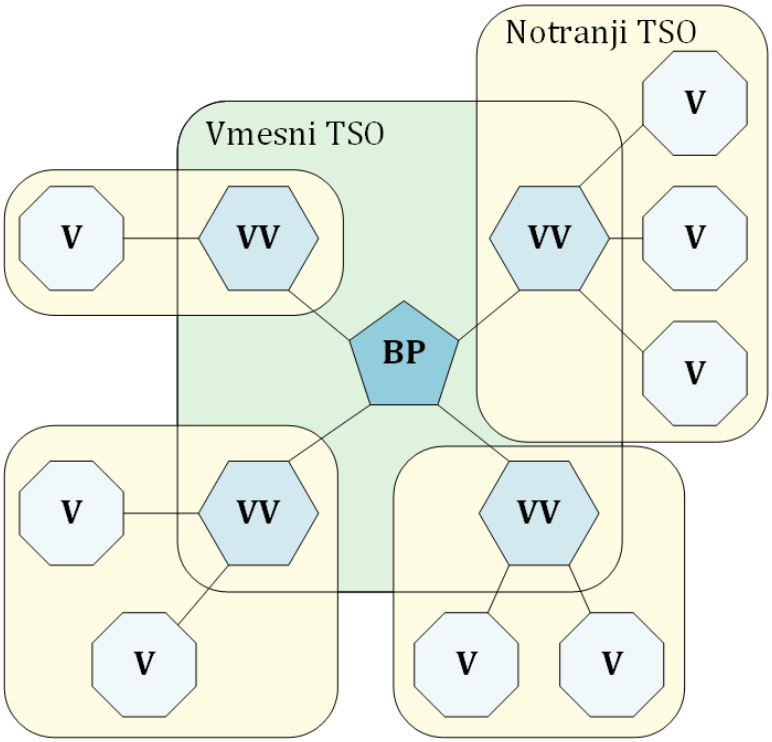
To poglavje je namenjeno predstavitvi novega protokola za overjanje in dogovor o ključu, primernega za uporabo v TSO. Novi protokol bomo v nadaljevanju naslavljali kot protokol II. Po klasifikaciji, predstavljeni v poglavju 4.3, spada protokol II med tradicionalne protokole. Protokol II zagotavlja medsebojno overjanje, pri katerem obe napravi v komunikaciji preverita istovetnost druga druge. Spada med protokole dogovora o ključu, ker se sejni ključ izdela na podlagi prispevkov obeh deležnikov vzpostavitve ključa. Protokol II je lahek protokol, ker za svoje delovanje uporablja samo zgoščevalno funkcijo in bitno operacijo XOR. Zagotavlja nesledljivost senzorskih vozlišč med ločenimi sejami ter je varen in učinkovit protokol za overjanje in dogovor o ključu v TSO.

Protokol II se od protokola I razlikuje v nekaj pomembnih točkah. Protokol II je namenjen varovanju komunikacije med senzorskimi napravami in bazno postajo, medtem ko je protokol I namenjen varovanju komunikacije do strežnika v zdravstvenem centru. Edinstvena struktura protokola I, ki uporablja tretje entitete, kot posrednike v procesu vzpostavitve ključa, je druga večja razlika, ki je tudi vsaj delno odgovorna, da je protokol II v primerjavi s protokolom I bolj pomnilniško, računsko in komunikacijsko učinkovit. Protokol I ne zagotavlja obojestranskega overjanja in čeprav sta oba protokola lahka, se v protokolu I uporablja tudi simetrično šifriranje, ki v protokolu II ni prisotno. Zadnja velika razlika je način vzpostavitve ključa, ki je v primeru protokola II dogovor o ključu, medtem ko protokol I zagotavlja samo prenos ključa.

Rezultati tega poglavja, vključno z novim protokolom II, analizo njegove varnosti in učinkovitosti, so povzeti po objavljenem članku z naslovom *A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs* [212] v reviji *Computer Networks*.

Protokol II je namenjen delovanju v dvonivojski zvezdni topologiji. V takšni strukturi sodelujejo tri vrste naprav. Drugonivojske naprave so senzorska vozlišča (V), ki so nameščena na telo in/ali v telo uporabnika. Te naprave imajo strogo omejene strojne vire in zaloge električne energije. Pri razvoju novega protokola, primernega za delovanje v TSO, je zato potrebno upoštevati predvsem zmogljivosti teh naprav. Prvonivojske naprave so vmesna vozlišča (VV), kot so na primer pametne ure ali pametni telefon. Tudi te naprave lahko pridobivajo in pošiljajo fiziološke ali druge podatke o stanju uporabnika. Prvonivojske naprave vsebujejo večje procesne, pomnilniške, komunikacijske in energetske zmogljivosti in so zato tudi primerne za delovanje kot posrednik med manj zmogljivimi senzorskimi vozlišči in bazno postajo. Bazna postaja (BP) ali lokalni strežnik je tretja vrsta naprave v topologiji. BP je veliko

zmogljivejša naprava kot V in VV in je odgovorna za zbiranje podatkov večjega števila senzorskih naprav in njihovega pošiljanja strežnikom v zdravstvenem centru. Senzorsko vozlišče V lahko zbrane podatke pošilja neposredno bazni postaji ali pa preko VV. Če želi VV poslati podatke BP, to stori na enak način kot V, le brez uporabe posrednika. Strežnik in BP sta zmogljivi napravi, zato je varovanje komunikacije ter overjanje entitet v tem delu komunikacije izven obsega protokola II. Varnost se lahko doseže z drugimi že dobro vzpostavljenimi protokoli. Omrežni model, v katerem deluje protokol II, je predstavljen na naslednji sliki (Slika 7.1). Enako omrežno topologijo uporabljata tudi protokola, predstavljena v člankih [90, 123]. Oba bosta zato v nadaljevanju uporabljena za primerjavo z novim protokolom II. Skoraj identična topologija je bila uporabljena tudi v protokolih [75, 114], vendar v teh protokolih komunikacija med V in BP obvezno poteka preko VV.



Slika 7.1: Omrežni model TSO za predlagani protokol overjanja in dogovora o ključu [90].

Pri razvoju protokola II in za namene analize varnostnih lastnosti protokola II je uporabljen naslednji model groženj (angl. threat model ali adversary model):

- Za BP se predpostavi, da je zaupanja vredna in ne bo kompromitirana.
- Napadalec lahko prosto prisluškuje prometu, vključi nova sporočila v komunikacijo in ponovno pošlje stara sporočila, ki so že bila dostavljena.
- Za V se predpostavi, da iz stroškovnih omejitev nima strojne opreme, odporne na nedovoljeno dostopanje. Če napadalec kompromitira vozlišče, lahko zato iz vozlišča pridobi vse podatke, shranjene na napravi.
- Komunikacijski kanal med napravami ni varen in senzorske naprave (V in VV) tipično niso zaupanja vredne.

V nadaljevanju tega poglavja bomo uporabljali številne okrajšave deležnikov in vrednosti, ki opisujejo delovanje protokola II. Seznam uporabljenih okrajšav oziroma simbolov je predstavljen v naslednji tabeli (Tabela 7.1) skupaj z opisi njihovega pomena.

Tabela 7.1: Definicija okrajšav, uporabljenih v poglavju 7.

Simbol	**Opis**
SA	Skrbnik sistema
V	Senzorsko vozlišče
BP	Bazna postaja
VV	Vmesno vozlišče
id_V	Identiteta in hkrati skrivni ključ senzorskega vozlišča V
id'_{VV}	Kratka identiteta vmesnega vozlišča VV
tid_V	Začasna identiteta vozlišča V in parameter celovitosti
k_{BP}	Glavna skrivnost lokalnega strežnika BP
k_V	Začasna skrivnost, ki jo zgradi BP za V
k_{V1}, k_{V2}	Zadnji poslan in zadnji prejet k_V^+ oz. k_V na bazni postaji BP
r_V	Začasen skrivni parameter, ki ga ustvari vozlišče V
a_V, b_V, x_V	Parametri overjanja
β	Parameter celovitosti
α, η, μ	Parametri overjanja, ki jih ustvari BP
t_V	Časovni žig, ki ga ustvari vozlišče V
k_S	Sejni ključ, ki je vzpostavljen ob koncu protokola II
$h(\cdot)$	Kriptografska zgoščevalna funkcija
$\|\|$	Operacija spajanja oz. konkatenacija
$\oplus$	Bitna operacija XOR
$X \rightarrow Y: M$	Entiteta X pošlje sporočilo M entiteti Y
X^*	Parameter X je bil izračunan, vendar njegova celovitost še ni bila preverjena
X^+	Parameter X, ki bo uporabljen ob naslednjem dogovoru o ključu

7.1 Nov protokol za overjanje in dogovor o ključu v telesnih senzorskih omrežjih

V tem poglavju je predstavljen nov protokol II. Sestavljen je iz treh faz. Fazi inicializacije in registracije sta izvedeni s strani skrbnika sistema (angl. system administrator – SA) v varnem okolju, ko naprave niso povezane v omrežje. Faza inicializacije je namenjena inicializaciji vrednosti na BP. V fazi registracije SA registrira vozlišča V in vmesna vozlišča VV na BP ter vzpostavi njihove predporazdeljene vrednosti. Faza overjanja in dogovora o ključu se izvede na odprtem omrežju. V tej fazi protokola se V in BP medsebojno overita in dogovorita o ključu,

s katerim bosta šifrirala vsa nadaljnja sporočila v tej seji. Glede na povezljivost V z BP poteka protokol overjanja in dogovora o ključu preko VV.

7.1.1 Faza inicializacije

V fazi inicializacije SA TSO preko varne povezave, v kateri ni mogoče prisluškovanje ali kakršnokoli poseganje v komunikacijo, inicializira vrednosti na BP, tako da:

I. Ustvari naključno glavno skrivnost BP – k_{BP}.
II. Shrani k_{BP} v pomnilnik BP.

7.1.2 Faza registracije

Faza registracije tudi poteka preko varnega kanala. SA registrira vozlišče V na BP, tako da:

I. Izbere unikatno identiteto id_V za senzorsko vozlišče V.
II. Izbere k_V za vozlišče V.
III. Izračuna $x_V = h(k_{BP} \,||\, k_V)$ in $a_V = k_{BP} \oplus k_V \oplus id_V$.
IV. V primeru, da je vozlišče V prvonivojska naprava, SA izbere dodatno unikatno identiteto id'_V.
V. Shrani parametre $\langle id_V, x_V, a_V \rangle$, če je naprava drugonivojska (V), ali parametre $\langle id'_V, id_V, x_V, a_V \rangle$, če je naprava prvonivojska (VV).
VI. Shrani parametre $\langle k_{BP}, k_{V1}, id_V \rangle$ za drugonivojsko napravo ter parametre $\langle k_{BP}, id'_V, k_{V1}, id_V \rangle$ za prvonivojsko napravo v pomnilnik BP, kjer je k_V shranjen kot k_{V1} in je k_{BP} že prisoten iz faze inicializacije.

7.1.3 Faza overjanja in dogovora o ključu

V tej fazi se senzorsko vozlišče V anonimno overi in dogovori o ključu z bazno postajo BP. Komunikacija lahko poteka neposredno med napravama ali pa se overjanje in dogovor o ključu izvedeta preko vmesnega vozlišča VV. Faza se v celoti izvede preko javnega kanala, kjer lahko zlonamerni akterji prisluškujejo ali vplivajo na komunikacijo. Potek izmenjave sporočil ter delovanje deležnikov faze overjanja in dogovora o ključu sta predstavljena na sliki po podrobnejšem opisu delovanja faze (Slika 7.2). Faza overjanja in dogovora o ključu se izvede po naslednjem postopku:

I. $V \rightarrow VV$: $\langle tid_V, a_V, b_V, t_V \rangle$. Pred tem V:
   - Izbere naključen r_V.
   - Ustvari časovni žig t_V.
   - Izračuna $b_V = x_V \oplus r_V$.
   - Izračuna $tid_V = h((id_V \oplus t_V) \,||\, r_V)$.

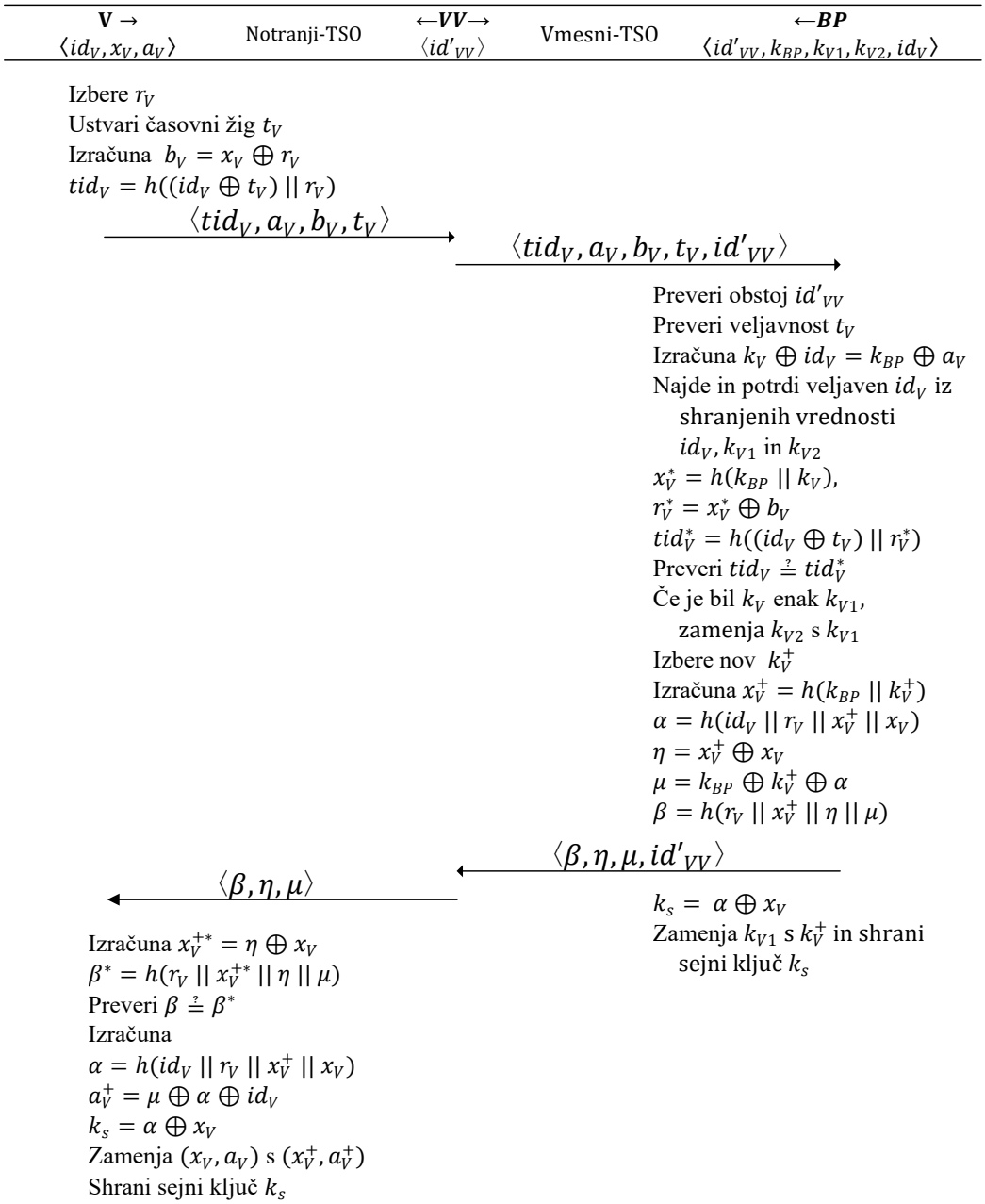
II. $VV \rightarrow BP$: $\langle tid_V, a_V, b_V, t_V, id'_{VV} \rangle$.
   - Ko komunikacija poteka preko VV, ta ne spremeni prejetega sporočila. Na konec sporočila le doda svojo identiteto vmesnega vozlišča id'_{VV} in posreduje sporočilo BP. Ko komunikacija ne vključuje VV se sporočila pošljejo neposredno med V in BP.

III. $BP \rightarrow VV$: $\langle \beta, \eta, \mu, id'_{VV} \rangle$. Potem ko sprejme sporočilo $\langle tid_V, a_V, b_V, t_V, id'_{VV} \rangle$, sledi BP naslednjemu zaporedju korakov:
   - Preveri, da ima v seznamu veljavnih VV zapis id'_{VV}. Prekine izvajanje, če ga nima. Ta korak je preskočen v primeru, da v komunikacijo ni vključeno VV.
   - Preveri veljavnosti časovnega žiga t_V, tako da preveri, če je bilo sporočilo poslano znotraj dovoljene časovne razlike $\Delta t = t^* - t_V$, kjer je t^* čas, ob katerem je BP prejela sporočilo $\langle tid_V, a_V, b_V, t_V, id'_{VV} \rangle$.
   - Izračuna $temp = k_V \oplus id_V = k_{BP} \oplus a_V$. Vrednost posameznih parametrov k_V in id_V v tej točki še ni znana BP.
   - Poišče shranjeno kombinacijo id_V in k_{V1} ali k_{V2}, tako da jih združi z operacijo XOR ($temp \stackrel{?}{=} (k_{V1} \oplus id_V$ ali $k_{V2} \oplus id_V)$). Če ne najde enake vrednosti, prekine izvajanje. Če najde ustrezno vrednost, pridobi posamezno vrednost obeh parametrov id_V in k_V (ustrezen od parametrov k_{V1} in k_{V2}).
   - Izračuna $x_V^* = h(k_{BP} \,||\, k_V)$ in $r_V^* = x_V^* \oplus b_V$.
   - Izračuna $tid_V^* = h((id_V \oplus t_V) \,||\, r_V^*)$.
   - Preveri, da je $tid_V \stackrel{?}{=} tid_V^*$. V primeru, da vrednosti nista enaki, BP preveri, če obstaja druga kombinacija id_V in k_{V1} ali k_{V2}, ki ustreza vrednosti $k_V \oplus id_V$, sicer prekine izvajanje.
   - Če je bil prejeti k_V enak vrednosti, shranjeni v parametru k_{V1}, se v parameter k_{V2} vpiše vrednost k_{V1}.
   - Izbere nov k_V^+.
   - Izračuna $x_V^+ = h(k_{BP} \,||\, k_V^+)$.
   - Izračuna $\alpha = h(id_V \,||\, r_V \,||\, x_V^+ \,||\, x_V)$.
   - Izračuna $\eta = x_V^+ \oplus x_V$.
   - Izračuna $\mu = k_{BP} \oplus k_V^+ \oplus \alpha$.
   - Izračuna $\beta = h(r_V \,||\, x_V^+ \,||\, \eta \,||\, \mu)$.
   - V tej točki lahko BP že pošlje odgovor $\langle \beta, \eta, \mu, id'_{VV} \rangle$ na prejeto sporočilo.
   - Shrani vrednost k_V^+ v parameter k_{V1}. Izračuna in shrani nov sejni ključ $k_S = \alpha \oplus x_V$. Parameter α je zgrajen med drugim tudi iz parametrov r_V in x_V^+. Prvega je prispevalo V, medtem ko je drugega ustvaril BP. Ker obe entiteti, med katerima se vzpostavlja varna komunikacija, prispevata vrednosti, od katerih je odvisen zgrajen sejni ključ, je to protokol za dogovor o ključu.

IV. $VV \rightarrow V$: $\langle \beta, \eta, \mu \rangle$.
   - Tako kot prej VV ne spreminja vsebine prejetega sporočila. Iz sporočila odstrani svoj identifikacijski parameter in ga posreduje V.

V. V prejme sporočilo $\langle \beta, \eta, \mu \rangle$ in:

- Izračuna $x_V^{+*} = \eta \oplus x_V$.
- Izračuna $\beta^* = h(r_V \,||\, x_V^{+*} \,||\, \eta \,||\, \mu)$.
- Preveri, da je $\beta \stackrel{?}{=} \beta^*$. Če obe vrednosti nista enaki, prekine izvajanje.
- Izračuna $\alpha = h(id_V \,||\, r_V \,||\, x_V^+ \,||\, x_V)$.
- Izračuna $a_V^+ = \mu \oplus \alpha \oplus id_V$.
- Izračuna in shrani nov sejni ključ $k_S = \alpha \oplus x_V$.
- Zamenja vrednosti parametrov (x_V, a_V) z vrednostmi (x_V^+, a_V^+).



Slika 7.2: Faza overjanja in dogovora o ključu novega protokola II [212].

7.2 Varnostna analiza protokola II

To poglavje je namenjeno analizi varnosti novega protokola II. Za vrednotenje varnosti je bila uporabljena hevristična metoda. Analiza je razdeljena na manjše sklope. V vsakem bo predstavljena varnostna lastnost, ki jo protokol II izpolnjuje, ali oblika napada, na katero je protokol II odporen. Poleg tega bo podana tudi razlaga, zakaj oziroma kako protokol doseže te lastnosti oziroma odpornosti.

Zaupnost in napad prisluškovanja

Prisluškovalec lahko zajame vsa sporočila, ki se pošiljajo preko javnega omrežja (vsa sporočila v fazi overjanja in dogovora o ključu). Napadalec lahko na takšen način zbere vrednosti naslednjih parametrov: tid_V, a_V, b_V, t_V, id'_{VV}, β, η, in μ. Tudi ob poznavanju vseh teh vrednosti napadalec ne more pridobiti nobene od skritih vrednosti (id_V, x_V, k_V, k_V^+ in k_{BP}). Parameter id'_{VV} ni skriven in se ne uporablja drugače kot za identifikacijo posrednika v komunikaciji. Vrednosti parametrov tid_V in β sta zaščiteni zaradi enosmernosti zgoščevalne funkcije, na podlagi katere sta nastali (in ker napadalec ne pozna vseh vhodnih vrednosti). Ostale vrednosti, ki se pošiljajo preko nezavarovane povezave, so vse sestavljene iz več vrednosti, ki so združene v končno vrednost z operacijo XOR. Uporabljene vrednosti niso javno znane (niti jih prisluškovalec ne more pridobiti) ter so uporabljene na takšen način, da ni mogoče ob združevanju (z operacijo XOR) različnih parametrov, ki so javno poslani, pridobiti nobene uporabljene posamezne vrednosti (id_V, x_V, r_V, x_V^+, k_{BP}, k_V, in k_V^+). Posledično prisluškovalec ne more razkriti dogovorjenega sejnega ključa. Zaupnost vseh skrivnih parametrov je tako ohranjena in protokol II je odporen na napade prisluškovanja.

Medsebojno overjanje in celovitost

Protokol II zagotavlja napravama, ki želita vzpostaviti ključ, medsebojno overjanje in preverjanje celovitosti izmenjanih sporočil. Overjanje V se opravi na podlagi parametra id_V, ki ga poleg V pozna samo še BP. Identiteta se prenese v parametru a_V. Izdelava začasne identitete tid_V je nemogoča brez poznavanja id_V, ki pa jo, kot je bilo omenjeno, poznata samo V in naslovnik sporočila (BP). BP preveri identiteto pošiljatelja, tako da primerja prejeto začasno identiteto z začasno identiteto, ki jo zgradi sam ($tid_V \stackrel{?}{=} tid_V^* = h((id_V \oplus t_V) \,||\, r_V^*)$) s pomočjo identitete V, ki jo izlušči iz parametra a_V, in s pomočjo lastnega seznama legitimnih identitet. V overi BP na posreden način. V sporočilu, ki ga V pošlje BP, se nahaja prameter b_V, ki ima vrednost $x_V \oplus r_V$. Parameter r_V je naključna vrednost, ki jo je ustvarilo V. Da lahko nekdo pridobi to vrednost iz parametra b_V, mora poznati x_V. Parameter x_V ustvari BP s pomočjo glavne skrivnosti k_{BP}. Zato lahko pravilen parameter x_V ustvari samo BP, ki lahko zatem tudi izlušči vrednost r_V iz parametra b_V. Senzorsko vozlišče V se prepriča, ali je pošiljatelj povratnega sporočila (predvidoma BP) pridobil pravilno vrednost parametra r_V s preverjanjem prejetega parametra β. V ustvari svoj β^* z uporabo vrednosti r_V, ki jo je posredovalo BP, in primerja ustvarjeno vrednost s prejeto vrednostjo ($\beta \stackrel{?}{=} \beta^* = h(r_V \,||\, x_V^{+*} \,||\, \eta \,||\, \mu)$). Če sta vrednosti enaki, to pomeni, da je bila pri izgradnji β uporabljena ista vrednost r_V, kot jo je vozlišče V posredovalo BP.

Ista parametra (tid_V in β), skrbita tudi za zagotavljanje celovitosti sporočil. V protokolu II se overjanje opravi istočasno kot preverjanje celovitosti sporočil. Parameter β je sestavljen iz vseh preostalih delov sporočila, ki ga varuje pred spremembami in dodatnimi vrednostmi, ki niso javno poslane. Posledično napadalec ne more spremeniti nobenega od parametrov, poslanih v sporočilu, ne da bi se ta sprememba zaznala ob preverjanju celovitosti ($\beta \stackrel{?}{=} \beta^*$). Isto velja tudi za tid_V, le da ta parameter posredno vključuje nekatere vrednosti, ki jih ščiti. V sporočilu, ki ga V pošlje ob začetku protokola II, se nahajajo vrednosti (a_V in b_V), ki niso vključene v $tid_V = h((id_V \oplus t_V) \,||\, r_V)$. Parametra a_V in b_V sta medij za varen prenos vrednosti id_V in r_V, ki pa sta vključeni v izdelavo tid_V. Kakršne koli spremembe v vrednostih parametrov a_V ali b_V bi vplivale na vrednosti id_V ali r_V, ki jih BP izlušči iz poslanih parametrov, in posledično bi preverjanje celovitosti $tid_V \stackrel{?}{=} tid_V^*$ zaznalo spremembe tudi v parametrih a_V in b_V. Celovitosti za kratko identiteto vmesnega vozlišča (id'_{VV}) ni potrebno zagotavljati.

Anonimnost in nepovezljivost sej

Protokol II zagotavlja anonimne in nepovezljive seje. Identiteta id_V se pošlje preko javne povezave v parametrih a_V in tid_V. Oba parametra v izgradnji vključujeta naključne vrednosti, ki se spremenijo ob vsaki uspešni vzpostavitvi seje (k_V) ali ob vsakem poizkusu vzpostavitve nove seje (r_V). Rezultat takšnega delovanja so vrednosti parametrov a_V in tid_V, ki so različne ob vsakem izvajanju protokola II in zato med zaporednimi vrednostmi istega parametra ne obstaja povezava. Iz vsebine poslanih sporočil zato ni mogoče razbrati identitete pošiljatelja in posledično protokol II zagotavlja anonimnost. Dinamično spreminjanje začasne identitete tid_V, a_V ter tudi vseh ostalih parametrov, ki so vključeni v sporočila, zagotavlja tudi, da v sporočilih ne ostaja pokazatelj, ki bi nakazoval na to, ali sporočila prihajajo od istega V. Kot rezultat nepovezljivosti sej prisluškovalec iz množice sporočil za dogovor o ključu ne more izločiti sporočil, ki jih je ustvarila ista naprava (V). To je mogoče, ker vse poslane vrednosti vsebujejo naključen parameter, ki je unikaten ob vsakem izvajanju protokola II. Parametrov, ki se vzpostavijo v eni in nato uporabijo v naslednji seji (vrednost $k_{BP} \oplus k_V$ in parameter x_V), tudi ni mogoče izluščiti ali drugače izkoristiti (z uporabo operacije XOR manipulirati javne parametre na način, ki producira konstantne vrednosti v zaporednih sejah). Tak pristop je mogoč za povezovanje zaporednih sej v protokolu Li in drugi [90], s katerim bo v nadaljevanju primerjana učinkovitost protokola II [212].

Napad s ponavljanjem

Prvo sporočilo v komunikaciji je zaščiteno pred napadom s ponavljanjem z uporabo časovnega žiga t_V. Če sporočilo prispe do naslovnika z večjo časovno zamudo od predvidene, se sporočilo zavrne. Časovno okno za sprejetje sporočila je zelo majhno, tako da napadalec nima dovolj časa zajeti in ponovno poslati sporočila na način, da bi lahko ogrozilo varnost protokola overjanja in dogovora o ključu ali ustvarilo drugo korist napadalcu. Časovni žig t_V je vključen tudi v tid_V, ki zagotavlja celovitost sporočila, tako da napadalec časovnega žiga ne more spremeniti, ne da bi bilo to takoj očitno prejemniku sporočila. Povratno sporočilo, ki ga BP pošlje V, varno vključuje naključno vrednost r_V. To vrednost je ustvarilo vozlišče V in ga na varen način (nihče razen naslovnika ne more razkriti te vrednosti) posredovalo BP. Če povratno sporočilo

vključuje različno vrednost (npr. vrednost, ki je bila uporabljena ob prejšnjem izvajanju protokola in jo je napadalec ponovil skupaj s sporočilom iz prejšnje seje), se sporočilo zavrže. Potem ko V sprejme ustrezno sporočilo (takšno, ki vključuje pravi r_V), se protokol zaključi in naprava ne sprejema več takšnih sporočil.

Napad poosebljanja senzorskega vozlišča in napad zajetja senzorskega vozlišča

Napad poosebljanja senzorskega vozlišča V je uspešen, ko napadalec ustvari veljavno sporočilo $\langle tid_V, a_V, b_V, t_V \rangle$. Da bi to bilo mogoče, mora napadalec poznati vrednosti id_V in x_V, ki pa jih, kot je že bilo omenjeno, ni mogoče pridobiti z napadom prisluškovanja. Druga možnost, ki jo ima napadalec na voljo, je pridobitev teh vrednosti iz zajete naprave. Kompromitirano vozlišče V bi omogočalo napadalcu poosebljanje zajetega V in uspešno overjanje pri BP. To je ena od slabih lastnosti vseh protokolov vzpostavitve ključa, ki hranijo trajne skrivnosti. Kljub temu protokol II preprečuje, da bi zajetje ene ali poljubnega števila V ogrozilo glavno skrivnost bazne postaje (k_{BP}). V hrani glavno skrivnost k_{BP} v parametrih x_V in a_V. V obeh primerih je k_{BP} varovana z enkratno in naključno vrednostjo k_V, ki jo ustvari BP. V prvem primeru je k_{BP} varovan zaradi enosmernosti zgoščevalne funkcije ($x_V = h(k_{BP}||k_V)$), medtem ko jo v drugem primeru ščiti operacija XOR, pri kateri je nemogoče na podlagi izhoda operacije razkriti vhodna niza ($a_V = k_{BP} \oplus k_V$). Edina možnost, ki preostane napadalcu za razkritje k_{BP}, je napad z grobo silo (angl. brute force attack), ki pa ga lahko izvede tudi brez zajetja V. Kot rezultat takšnega delovanja lahko napadalec zajame poljubno število V in s tem ne bo v nobeni meri izboljšal verjetnosti uspešnega napada na katero koli drugo, še nekompromitirano vozlišče V. Glede na to, da se V nahaja v TSO, kjer je relativno preprosto opaziti, če je bila senzorska naprava odtujena, se lahko takšna naprava tudi hitro odstrani s seznama legitimnih vozlišč na BP in se tako omejijo posledice zajetja V.

Napad poosebljanja bazne postaje in napad zajetja bazne postaje

Podobno kot v napadu poosebljanja senzorskega vozlišča mora napadalec za uspešno poosebljanje bazne postaje BP ustvariti veljavno sporočilo $\langle \beta, \eta, \mu \rangle$. Vse vrednosti v sporočilu so sestavljene iz glavne skrivnosti BP k_{BP} in začasne skrivnosti k_V. Oba parametra sta poznana samo BP, zato je nemogoče, da bi napadalec lahko poosebljal BP, ne da bi predčasno pridobil dostop do te naprave. Za napravo, ki se uporablja za BP, se predpostavlja, da je zmogljiva in ima strojno opremo, ki preprečuje nedovoljen dostop. Napadalec, ki zajame BP, zato ne bi mogel iz naprave pridobiti hranjenih skrivnih vrednosti. Če takšne zaščite ni in napadalec uspešno pridobi hranjene vrednosti, protokol II izgubi zmožnost varnega overjanja in vzpostavitve ključa.

Prihodnja varnost in pretekla varnost sejnih ključev

V znanstveni literaturi, ki opisuje protokole vzpostavitve ključa v TSO, smo zasledili, da se v hevrističnih analizah varnosti lahkih tradicionalnih protokolov uporablja prihodnja in pretekla varnost sejnih ključev (npr. [90, 123]) namesto trajnih ključev, kot je to zapisano v definiciji, ki je bila predstavljena v poglavju 4.1. Lastnost, kot je v osnovi opredeljena, je namreč nedosegljiva v sistemih, v katerih varnost temelji na trajnem ključu, namenjenem uporabi v

simetrični kriptografiji (brez uporabe asimetrične kriptografije, fizioloških podatkov ipd.). Prihodnja varnost in pretekla varnost sejnih ključev je zato lastnost sistema, ki preprečuje, da se ob razkritju sejnega ključa ogrozi varnost predhodno oziroma v prihodnje uporabljenih sejnih ključev.

V protokolu II se sejni ključ k_S ustvari iz vrednosti parametrov α in x_V. V izračun obeh parametrov so vključene začasne vrednosti (r_V in k_V), tako da je ustvarjeni k_S naključen vsako sejo in nima nič skupnega s predhodnimi ali naslednjimi sejnimi ključi. Zato protokol II izpolnjuje načelo prihodnje in pretekle varnosti sejnih ključev. V primeru, da bi napadalcu uspelo na kak način ugotoviti sejni ključ, poleg tega da iz njega ne more sklepati o prihodnjih ali preteklih ključih, na njegovi podlagi tudi ni mogoče pridobiti vrednosti parametrov α in x_N, iz katerih je zgrajen. Dodatno sta tudi parametra zgrajena s pomočjo zgoščevalne funkcije, tako da tudi če napadalec slučajno ugane katero od vrednosti, še vedno ne more s tem razkriti dolgotrajnih skrivnosti (id_V in k_{BP}).

Napad vrinjenega napadalca

Napad vrinjenega napadalca omogoča napadalcu, da prestreza sporočila med napravama, ki želita vzpostaviti ključ, in deluje kot posrednik v njuni komunikaciji, ne da bi katera od naprav zaznala, da ne komunicira z dejanskim naslovnikom. Napad vrinjenega napadalca se prepreči z medsebojnim overjanjem oziroma nezmožnostjo poosebljanja naprav v komunikaciji. Posledično napad vrinjenega napadalca v protokolu II ni mogoč.

Napad desinhronizacije

Napad desinhronizacije je mogoč, ko mora več entitet vzdrževati enako stanje. V protokolu II takšno stanje predstavlja parameter k_V. Čeprav mogoče ni takoj očitno, morata ta parameter v enaki obliki hraniti V in BP. V ga hrani kot del parametra a_V, medtem ko se v BP hrani v parametrih k_{V1} (zadnji k_V^+, ki ga je BP ustvaril in poslal V) in k_{V2} (zadnji k_V, ki ga je BP prejel od V). Uporaba hranjenja obeh oblik parametrov je potreba, ker bi sicer protokol II bil dovzeten za napad desinhronizacije.

Če BP ne hrani drugega parametra k_{V2} in po definiranem delovanju ustvari nov k_V^+, ki ga shrani v parameter k_{V1} ter pošlje v sporočilu vozlišču V, in če zatem napadalec ali napaka v omrežju prepreči dostavo tega sporočila, bi ob naslednjem izvajanju protokola II V poslal sporočilo, ki bi vsebovalo parametre (a_V in b_V), ustvarjene na podlagi starega k_V (ker novi parametri, zgrajeni z vrednostjo k_V^+, niso bili nikoli dostavljeni vozlišču V). BP bi v tem primeru iz prejetih vrednosti poizkusil pridobiti vrednosti id_V in k_V, vendar bi bil pri tem neuspešen, ker shranjena vrednost v parametru k_{V1} ne bi ustrezala prejeti vrednosti k_V (k_V je prejet kot del parametra a_V). Kot posledica tega se V ne bi več mogel overiti pri BP, dokler se ne bi določene dolgotrajne vrednosti na eni od naprav ročno popravile. Zato da se takšen napad prepreči, BP hrani dva parametra. Prvi (k_{V1}) hrani najnovejšo začasno skrivnost k_V^+, ki jo je BP ustvaril in posredoval V, medtem ko se v drugem parametru (k_{V2}) hrani najnovejša začasna skrivnost k_V, za katero je BP prepričan, da jo V pozna (tj. najnovejša začasna skrivnost k_V, ki jo je BP prejel od V). Ob hranjenju obeh vrednosti situacija, v kateri povratno sporočilo od BP ne prispe do V,

ne povzroči desinhronizacije, saj se V lahko naslednjič uspešno overi tudi z uporabo starejših vrednosti parametrov. Takšno delovanje nekoliko poveča porabo pomnilnika na BP, vendar to ni težava, saj gre za zmogljivo napravo. Na napad desinhronizacije je med drugim dovzeten tudi protokol Ibrahim in drugi [123], s katerim bomo v nadaljevanju primerjali učinkovitost protokola II. Uporaba shranjevanja začasne skrivnosti v dveh parametrih bi tudi v protokolu Ibrahim in drugi [123] preprečila možnost takšnega napada.

7.3 Analiza učinkovitosti protokola II

To poglavje je namenjeno analizi učinkovitosti novega protokola II in njegovi primerjavi s sorodnimi protokoli. Protokol II bo primerjan s protokolom Li in drugi [90] ter Ibrahim in drugi [123]. Vsi trije protokoli spadajo med lahke tradicionalne protokole in so relativno moderne rešitve (najstarejši je protokol Ibrahim in drugi, ki je bil predstavljen leta 2016). Vsi trije so protokoli za overjanje in dogovor o ključu ter so namenjeni delovanju v dvonivojski zvezdni topologiji, kot je opisana na začetku poglavja 7. Avtorji vseh treh protokolov predvidevajo enak model groženj. Vse te skupne lastnosti naredijo te tri protokole zelo primerljive med seboj. Učinkovitost protokolov bo ocenjena na podlagi merjenja porabe pomnilnika, računske zahtevnosti in stroškov komunikacije.

V namen analize porabe pomnilnika bomo uporabili velikost parametrov, kot so jih uporabili tudi avtorji v obeh protokolih, s katerima primerjamo novi protokol. Bazna postaja BP v protokolu II hrani kratko identiteto id'_{VV} dolžine 16 bitov za vsako vmesno vozlišče VV, ki je dodano v fazi registracije. Število VV, katerih identitete hrani BP, je označeno kot m. Vsi preostali parametri, ki jih hrani BP (k_{BP}, id_V, k_{V1}, k_{V2}, in k_S), so velikosti 160 bitov. Vsi ti parametri, z izjemo k_{BP}, ki je specifičen za vsako posamezno BP, so hranjeni v n izvodih, kjer je n število vozlišč V, ki so bila v fazi registracije dodana na BP. V protokolu II vozlišča V hranijo parametre id_V, x_V, a_V, in k_S, od katerih vsak zaseda po 160 bitov. Vmesna vozlišča VV hranijo enake parametre kot V, z dodatkom prej omenjene 16-bitne kratke identitete id'_{VV}. Zato ker so te vrednosti tako podobne drugonivojskim napravam in ker se ob posredovanju sporočil ne opravi nobena dodatna obdelava podatkov, smo te naprave izpustili iz tega dela analize. Izračuni celotne porabe pomnilnika na posamezni napravi v posameznih protokolih so predstavljeni v naslednji tabeli (Tabela 7.2).

Protokol Li in drugi je od vseh treh primerjanih protokolov najbolj učinkovit pri porabi pomnilnika BP. Protokol Ibrahim in drugi je manj učinkovit, vendar še vedno veliko bolj uspešen pri izrabi pomnilnika BP kot protokol II. V porabi pomnilnika na BP je torej novi protokol II izrazito najslabši. Pri tem je treba upoštevati, na kaj ta razlika v porabi pomnilnika vpliva oziroma zakaj je nastala. BP je zmogljiva naprava, ki ima ogromne količine pomnilnika, zato nekoliko večja poraba tega ni velik problem za napravo. Razlog za večjo porabo pomnilnika v primerjavi z ostalima protokoloma je predvsem izboljšanje odpornosti na nekatere napade. Za razliko od obeh predhodnih protokolov je protokol II odporen na napad sledenja (nepovezljivost sej) in napad desinhronizacije. Za namene preprečevanja sledenja

vozliščem iz seje v sejo se v protokolu II na BP hranita parametra id_V in k_{V1}, medtem ko je hranjenje parametrov k_{V1} in k_{V2} na BP potrebno za preprečevanje napada desinhronizacije. Pri tem je pomembno poudariti, da je protokol II za povečano varnost povečal porabo pomnilnika na BP, medtem ko je poraba pomnilnika na V primerljiva z drugima protokoloma. Vsi trije protokoli za svoje delovanje na V hranijo štiri parametre enake velikosti. Poraba pomnilnika na vozlišču V je enaka v vseh treh protokolih. Novi protokol II ima torej izboljšano odpornost na napade za ceno nekoliko povečane porabe pomnilnika na zmogljivi napravi, kjer so danes trajne pomnilniške kapacitete najcenejše od vseh komponent [213].

Vsi trije protokoli za overjanje in dogovor o ključu so lahki protokoli, ki za delovanje uporabljajo le funkcijo zgoščevanja in operacijo XOR. Na računsko zahtevnost protokolov v veliki meri vpliva samo uporaba zgoščevalnih funkcij, ki se veliko bolj zahtevne kot operacije XOR. Čeprav v analizi računske zahtevnosti upoštevamo tudi operacije XOR, je efektivna računska zahtevnost enaka številu zgoščevalnih funkcij, saj je v primerjavi računska zahtevnost operacij XOR zanemarljiva. Računska zahtevnost vseh treh protokolov je predstavljena v naslednji tabeli (Tabela 7.2). V njej je čas izvajanja zgoščevalne funkcije označen s t_h, medtem ko je čas izvajanja operacije XOR zapisan kot t_{XOR}. Med tremi protokoli je protokol Ibrahim in drugi najbolj računsko zahteven na vseh napravah, vključenih v protokol. Na BP je protokol Li in drugi najbolj učinkovit, medtem ko je novi protokol II srednje učinkovit med tremi primerjanimi protokoli. Število operacij XOR je v protokolu II variabilno glede na zahtevnost iskanja parametrov id_V in k_V. Postopek iskanja zahteva kombiniranje parametra id_V s parametroma k_{V1} in k_{V2} za vsako od n registriranih vozlišč V. Za to bo v povprečju potrebnih n operacij XOR (in dvakrat toliko operacij v najslabšem možnem primeru). V primeru, da so povratna sporočila konstantno uspešno dostavljena V (v komunikaciji ne prihaja do napak in napadalec ne vpliva na komunikacijo), se povprečno število potrebnih operacij XOR dodatno zmanjša na $\frac{n}{2}$, ker se lahko postopek iskanja optimizira tako, da se k_{V2} preverjajo naknadno, potem ko so bile preverjene vse začasne skrivnosti, hranjene v k_{V1}. To je mogoče, ker je parameter k_{V2} potreben za uspešno vzpostavitev ključa le v primeru, da V ni prejel nove vrednosti k_V^+, ki jo je generiral in poslal BP. Kljub temu da je lahko ob takem delovanju in večjem številu n potrebnih precej operacij XOR, je računska zahtevnost izvajanja zgoščevalne funkcije za en sam blok podatkov še vedno večja. Računska zahtevnost overjanja in dogovora o ključu na V je najmanj zahtevna ob uporabi protokola II, čeprav je ta zgolj za eno operacijo XOR bolj učinkovit kot protokol Li in drugi.

Tabela 7.2: Primerjava porabe trajnega pomnilnika in računske zahtevnosti novega protokola II s sorodnimi protokoli.

Protokol	Naprava	Poraba pomnilnika (bit)	Računska zahtevnost
Protokol Ibrahim in drugi [123]	V	640	$5t_h + 5t_{XOR} \approx 5t_h$
	BP	$480n + 160$	$8t_h + 4t_{XOR} \approx 8t_h$
Protokol Li in drugi [90]	V	640	$3t_h + 7t_{XOR} \approx 3t_h$
	BP	$16m + 160(n + 1)$	$5t_h + 12t_{XOR} \approx 5t_h$
Protokol II	V	640	$3t_h + 6t_{XOR} \approx 3t_h$
	BP	$640n + 16m + 160$	$5t_h + (n + 7)t_{XOR} \approx 5t_h$

Vrednotenje računske zahtevnosti je bilo opravljeno po vzoru analiz obeh protokolov, s katerima primerjamo novi protokol II. Ocene časa izvajanja in porabe električne energije računskih operacij so prikazane na spodnji tabeli (Tabela 7.3) in so bile narejene na podlagi meritev 32-bitnega mikrokontrolerja Cortex-M3 [214], katerega centralna procesna enota deluje s frekvenco 72 MHz. Takšna naprava izvede zgoščevalno funkcijo v 0,06 ms [75] in ima v aktivnem stanju porabo 118,8 mW [123]. Protokol II potrebuje za delovanje enako število zgoščevalnih funkcij kot protokol Li in drugi, zato so tudi njune ocene porabe časa in energije enake. Tako kot prej je v računski zahtevnosti protokol Ibrahim in drugi najmanj učinkovit.

Tabela 7.3: Primerjava časovne zahtevnosti računskih operacij in porabe električne energije novega protokola II s sorodnima protokoloma na 32-bitnem mikrokrmilniku Cortex-M3.

Protokol	Naprava	Čas izvajanja računskih operacij (ms)	Porabljena energija (mJ)
Protokol Ibrahim in drugi [123]	V	0,3	0,036
	BP	0,48	0,057
Protokol Li in drugi [90]	V	0,18	0,021
	BP	0,3	0,036
Protokol II	V	0,18	0,021
	BP	0,3	0,036

Učinkovitost komunikacije je v TSO zelo pomembna, saj ravno pošiljanje in prejemanje sporočil tipično predstavlja največji delež porabe energije. Ker vsi protokoli uporabljajo enak model omrežja in imajo enako število ter strukturo izmenjanih sporočil, je primerjava med njimi preprosta. Protokol II je v tej metriki vrednotenja učinkovitosti izrazito najboljši med tremi primerjanimi protokoli. Čeprav protokol II pošlje skupno najmanjšo količino podatkov od vseh protokolov, je protokol Ibrahim in drugi malenkostno bolj učinkovit pri izrabi virov vozlišča V. Protokol II v svojem delovanju izmenja najmanj podatkov z BP in je posebej učinkovit pri količini komunikacije z VV, ki je tudi strojno omejena naprava (čeprav ne v takšni meri kot V). Protokol Li in drugi je v vseh pogledih najmanj komunikacijsko učinkovit med primerjanimi protokoli. Količina podatkov v komunikaciji za vsak protokol in med vsemi napravami je

predstavljena v spodnji tabeli (Tabela 7.4), kjer je predpostavljena velikost vseh parametrov 160 bitov, z izjemo id'_{VV}, ki je 16-biten, in t_V, ki je dolg 32 bitov.

Tabela 7.4: Primerjava učinkovitosti komunikacije novega protokola II s sorodnimi protokoli.

Pošiljatelj → Prejemnik	**Strošek komunikacije**		
	Protokol Ibrahim in drugi [123] **(bit)**	**Protokol Li in drugi** [90] **(bit)**	**Protokol II (bit)**
$V \rightarrow VV$	480	672	512
$VV \rightarrow BP$	640	688	528
$BP \rightarrow VV$	640	656	496
$VV \rightarrow V$	480	640	480

8 Zaključek

Osrednji cilj doktorske disertacije je razvoj novega protokola za overjanje in dogovor o ključu, primernega za uporabo v brezžičnih telesnih senzorskih omrežjih, ki je varnejši in/ali učinkovitejši od primerljivih obstoječih rešitev. Poudarek v razvoju novega protokola je poleg varnosti predvsem na nezahtevnem delovanju. Razlog za to so manj zmogljive senzorske naprave, ki so sestavni del telesnih senzorskih omrežij. Skupaj z vsemi omejitvami v takšnih omrežjih so bile predstavljene tudi razlike s podobnimi omrežji. Naštete in opisane so bile tudi varnostne lastnosti, za katere je pomembno, da jih protokoli overjanja in vzpostavitve ključa izpolnjujejo. Sestavljen je bil tudi seznam pogostih napadov, na katere morajo biti takšni protokoli odporni (v kolikor je to smiselno za dane okoliščine).

Za namene ugotavljanja trenutnega stanja na področju protokolov vzpostavitve ključa, primernih za uporabo v TSO, je bil izveden pregled literature. Na podlagi pregleda in najdenih razlik v strukturi različnih protokolov vzpostavitve ključa v TSO je bila izdelana nova klasifikacija takšnih protokolov. Protokoli so bili razporejeni v skupino tradicionalnih, če uporabljajo pristop asimetrične kriptografije ali predporazdeljenih ključev. Tradicionalni protokoli so se izkazali za najpogostejšo obliko vzpostavitve ključa. Za skupino protokolov na osnovi fizioloških podatkov je značilno, da za svoje delovanje izrabljajo fiziološke signale uporabnika, na telesu katerega se naprave, ki izvajajo takšne protokole, nahajajo. Takšni protokoli tipično izrabijo fiziološke podatke za varovanje prenosa ključa. Protokoli z generiranjem skrivnega ključa uporabljajo okoliški signal, ki je skupen vsem napravam v omrežju, in tipično iz tega, za razliko od protokolov na osnovi fizioloških podatkov, neodvisno na ločenih napravah ustvarijo šifrirni ključ. Zadnja skupina so hibridni protokoli. Ti v enem protokolu združujejo več pristopov za vzpostavitev ključa, ki so sicer značilni za druge omenjene skupine. V veliko takšnih protokolih se združuje delovanje tradicionalnih protokolov in protokolov na osnovi fizioloških podatkov. S tem je bilo pokazano, da med protokoli vzpostavitve ključa, namenjenih TSO, obstajajo skupine protokolov, ki delujejo na podobnih principih, na podlagi katerih je mogoče vse obstoječe protokole klasificirati v posamezne skupine. S tem je bila potrjena prva hipoteza doktorske disertacije, ki se glasi:

Hipoteza 1: *Obstajajo ključne razlike v strukturi in lastnostih obstoječih protokolov za vzpostavitev ključa v TSO, na podlagi katerih je mogoče takšne protokole klasificirati v različne skupine.*

Med pregledom znanstvene literature je bila posebna pozornost posvečena tudi metodam, ki so jih avtorji protokolov uporabili za preverjanje varnosti in učinkovitosti svojih protokolov. Predstavljene so bile posamezne metode, pogostost njihove uporabe ter prednosti in slabosti vsake metode. Izkazalo se je, da so metode, ki se uporabijo za vrednotenje varnosti in učinkovitosti protokolov, v veliki meri odvisne od načina delovanja protokola. To pomeni, da klasifikacija protokola dobro nakazuje tudi metode, ki so primerne za vrednotenje njegove

varnosti in učinkovitosti. Najpogostejše metode vrednotenja učinkovitosti so zato tiste, ki so najbolj nevtralne glede na strukturo vrednotenih protokolov. V primeru analize varnosti se je kot najpogosteje uporabljen pristop izkazala hevristična metoda. Pregled analiz učinkovitosti je pokazal, da se tipično ne uporabi ena sama metoda, ampak se obravnava več ločenih vidikov učinkovitosti delovanja. Najpogostejši so poraba pomnilnika, računska zahtevnost, učinkovitost komunikacije in poraba električne energije. Te oblike vrednotenja varnosti in učinkovitosti so bile v nadaljevanju disertacije tudi uporabljene za analizo novih protokolov. V disertaciji sta bila predstavljena dva nova protokola za overjanje in vzpostavitev ključa, primerna za uporabo v TSO.

Protokol I je varnostno izboljšan obstoječ lahek protokol, ki za bolj varno delovanje žrtvuje nekaj učinkovitosti izvornega protokola. Konstrukcija protokola omogoča prelaganje zahtevnih računskih operacij s strojno zelo omejenih senzorskih vozlišč na tretje entitete, ki takšnih omejitev nimajo. Druga dobra lastnost takšnega delovanja je zakritje povezave med vozliščem in strežnikom, s katerim senzorsko vozlišče vzpostavi ključ, ne da bi pri tem razkrilo vzpostavljeno skrivnost tretjim entitetam, ki sodelujejo v protokolu. Po načinu delovanja se protokol I uvršča med tradicionalne. Analiza varnosti pokaže, da novi protokol I nadgradi izvorni protokol z izboljšanjem zagotavljanja zaupnosti in celovitosti izmenjanih sporočil in doda zaščito pred določenimi napadi poosebljanja, napadi s ponovitvijo, napadi za zavrnitev storitve itd. Protokol I tudi doda mehanizem, s katerim se lahko končni napravi v komunikaciji prepričata, da so se tretje entitete overile pri obeh končnih napravah. Vzpostavitev ključa preko tretjih entitet, ki niso nujno zaupanja vredne, omogoča napad zarote, v katerem tretje entitete sodelujejo z namenom razkritja posredovane skrivnosti. V nalogi so podana nekatera priporočila in predlogi, kako uporabiti predlagani protokol I, tako da se takšna tveganja zmanjšajo. Analiza učinkovitosti je pokazala, da so vse spremembe, ki so bile potrebne za izboljšanje varnosti, tudi nekoliko zmanjšale učinkovitost protokola I v primerjavi z izvornim protokolom. Vendar protokol I uvede tudi alternativno delovanje za primere, ko pri overjanju in vzpostavitvi ključa v komunikaciji ne pride do zaznavanja nedovoljenega posega v komunikacijo. V takšnem primeru se protokol izvede na preprostejši način, ki je učinkovitejši od izvornega protokola. Ne glede na to je kompromis med obema kazalnikoma kakovosti protokola pozitiven, saj je bila varnost protokola izboljšana v večji meri, kot je bila s tem prizadeta njegova učinkovitost. Čeprav je protokol I lahek, varen in sorazmerno učinkovit protokol, ki gradi na novi ideji izvornega protokola, to ni protokol dogovora o ključu, ker skrivnost v protokolu ustvari senzorsko vozlišče in je zatem samo posredovana strežniku preko tretjih entitet. Zato na podlagi tega protokola ne moremo v celoti potrditi druge hipoteze doktorske disertacije, ki se glasi:

Hipoteza 2: *S pomočjo rezultatov prve hipoteze je mogoče razviti nov protokol za overjanje in dogovor o ključu, ki je primeren za delovanje v TSO. Novi protokol zagotavlja varno delovanje glede na podane kriterije iz literature in je odporen na znane napade ter je učinkovit.*

Drugo hipotezo potrdimo s protokolom II. Protokol II je lahek protokol, saj za svoje delovanje uporablja le kriptografsko zgoščevalno funkcijo in operacijo XOR. Protokol II omogoča overjanje in dogovor o ključu, saj na nastalo vzpostavljeno skrivnost na nepredvidljiv način

vplivata oba deležnika v protokolu. Protokol II spada v najštevilčnejšo skupino tradicionalnih protokolov in je namenjen delovanju v dvonivojski zvezdni topologiji, kjer overjanje in dogovor o ključu poteka med senzorskim vozliščem in bazno postajo. Analiza varnosti je bila ponovno opravljena s hevrističnim modelom. Pokazala je, da protokol II izpolnjuje vse potrebne varnostne lastnosti in je odporen na tipične napade v takšnih omrežjih. Za namen analize učinkovitosti je bil protokol II primerjan z dvema sorodnima protokoloma iz literature. Analiza varnosti je pokazala, da je protokol II odporen tudi na nekatere napade (tj. napad sledenja in napad desinhronizacije), na katere protokola, uporabljena za primerjavo učinkovitosti, nista (na vsakega od protokolov je možen eden od omenjenih napadov). Analiza učinkovitosti je vsebovala vrednotenje porabe pomnilnika, računske zahtevnosti in učinkovitosti komunikacije. V primerjavi učinkovitosti z drugima dvema protokoloma se je protokol II izkazal kot zelo učinkovit, saj je v vseh pomembnih kazalnikih bil vsaj tako učinkovit kot preostala protokola ali pa celo bolj. Protokol II ima glede na primerjana protokola samo nekoliko večjo porabo pomnilnika na bazni postaji, toda ker to ni strojno omejena naprava, to ni pomemben dejavnik njegove učinkovitosti. Novi protokol II je zato varen in učinkovit protokol za overjanje in dogovor o ključu, primeren za uporabo v telesnih senzorskih omrežjih.

Literatura

[1] D. Kahn, The codebreakers: the story of secret writing, Scribner, 1996. http://www.simonandschuster.com/books/The-Codebreakers/David-Kahn/9780684831305 (dostopano 31. julij 2018.).

[2] N.G. McDonald, PAST, PRESENT, AND FUTURE METHODS OF CRYPTOGRAPHY AND DATA ENCRYPTION, b. d. https://pubweb.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf (dostopano 31. julij 2018.).

[3] B. Schneier, Applied cryptography : protocols, algorithms, and source code in C, 2nd editio, Wiley, 1996.

[4] C. Beebout, Why cryptography is essential to IoT security, http://iotdesign.embedded-computing.com. (2016). http://iotdesign.embedded-computing.com/guest-blogs/why-cryptography-is-essential-to-iot-security/ (dostopano 31. julij 2018.).

[5] J. Reimer, Personal Computer Market Share: 1975-2004, (b. d.). http://www.retrocomputing.net/info/siti/total_share.html (dostopano 31. julij 2018.).

[6] A. Ali, F.A. Khan, Key Agreement Schemes in Wireless Body Area Networks: Taxonomy and State-of-the-Art, J. Med. Syst. 39 (2015) 115. doi:10.1007/s10916-015-0272-9.

[7] V. Jones, A. van Halteren, I. Widya, N. Dokovsky, G. Koprinkov, R. Bults, D. Konstantas, R. Herzog, Mobihealth: Mobile Health Services Based on Body Area Networks, v: M-Health, Springer US, Boston, MA, 2006: str. 219–236. doi:10.1007/0-387-26559-7_16.

[8] IEEE 802.15 WPAN, Task Group 6, Body Area Networks, (b. d.). http://www.ieee802.org/15/pub/TG6.html (dostopano 3. april 2018.).

[9] UN, World Population Prospects: The 2015 Revision, Popul. Div. Dep. Econ. Soc. Aff. United Nations Secr. (2015). https://esa.un.org/unpd/wpp/.

[10] World Health Organization, Global status report on noncommunicable diseases 2010, 2011. http://www.who.int/nmh/publications/ncd_report2010/en/.

[11] R. G.K, K. Baskaran, A Survey on Futuristic Health Care System: WBANs, Procedia Eng. 30 (2012) 889–896. doi:10.1016/J.PROENG.2012.01.942.

[12] S.A. Salehi, M.A. Razzaque, I. Tomeo-Reyes, N. Hussain, IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view, v: 2016 22nd Asia-Pacific Conf. Commun., IEEE, 2016: str. 523–528. doi:10.1109/APCC.2016.7581523.

[13] Zakon o varstvu osebnih podatkov (ZVOP-1), Ur. List. (2007). https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/82668 (dostopano 16. februar 2017.).

[14] Splošna uredba o varstvu podatkov, (b. d.). https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679 (dostopano 31. maj 2018.).

[15] C.C.Y. Poon, A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health, IEEE Commun. Mag. 44 (2006) 73–81. doi:10.1109/MCOM.2006.1632652.

[16] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, V.C.M. Leung, Body Area Networks: A Survey, Mob. Networks Appl. 16 (2011) 171–193. doi:10.1007/s11036-010-0260-8.

[17] Shu-Di Bao, Lian-Feng Shen, Yuan-Ting Zhang, A novel key distribution of body area networks for telemedicine, v: IEEE Int. Work. Biomed. Circuits Syst. 2004., IEEE, 2004: str. 37–40. doi:10.1109/BIOCAS.2004.1454091.

[18] A. Pantelopoulos, N.G. Bourbakis, A Survey on Wearable Sensor-Based Systems for Health Monitoring and Prognosis, IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev. 40 (2010) 1–12. doi:10.1109/TSMCC.2009.2032660.

[19] P. Kumar, S.G. Lee, H.J. Lee, E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks, Sensors. 12 (2012) 1625–1647. doi:10.3390/s120201625.

[20] D. He, N. Kumar, J. Chen, C.C. Lee, N. Chilamkurti, S.S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimed. Syst. 21 (2013) 49–60. doi:10.1007/s00530-013-0346-9.

[21] X. Li, Z. Zheng, X. Zhang, A Secure Authentication and Key Agreement Protocol for Telecare Medicine Information System, v: 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol., IEEE, 2015: str. 275–281. doi:10.1109/NGMAST.2015.75.

[22] C.-T. Li, D.-H. Shih, C.-C. Wang, Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems, Comput. Methods Programs Biomed. 157 (2018) 191–203. doi:10.1016/J.CMPB.2018.02.002.

[23] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Comput. Networks. 54 (2010) 2787–2805. doi:10.1016/j.comnet.2010.05.010.

[24] D. Evans, The Internet of Things: How the Next Evolution of the Internet is Changing Everything, 2011. https://www.researchgate.net/publication/313420977_The_Internet_of_Things_How_the_Next_Evolution_of_the_Internet_is_Changing_Everything (dostopano 11. december 2018.).

[25] K.L. Lueth, State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating, (2018). https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (dostopano 11. december 2018.).

[26] Cisco, Internet of Things At a Glance - Cisco, (2016). https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf (dostopano 11. december 2018.).

[27] D.E. Kouicem, A. Bouabdallah, H. Lakhlef, Internet of things security: A top-down survey, Comput. Networks. 141 (2018) 199–221. doi:10.1016/J.COMNET.2018.03.012.

[28] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, Marrs, Disruptive technologies: Advances that will transform life, business, and the global economy, 2013. doi:10.1002/sres.

[29] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Comput. Networks. 52 (2008) 2292–2330. doi:10.1016/J.COMNET.2008.04.002.

[30] S.M. Mohamed, H.S. Hamza, I.A. Saroit, Coverage in mobile wireless sensor networks (M-WSN): A survey, Comput. Commun. 110 (2017) 133–150. doi:10.1016/J.COMCOM.2017.06.010.

[31] H. Zhao, R. Xu, M. Shu, J. Hu, Physiological-signal-based key negotiation protocols for body sensor networks: A survey, Simul. Model. Pract. Theory. 65 (2016) 32–44. doi:10.1016/j.simpat.2015.12.003.

[32] M. Al Ameen, J. Liu, K. Kwak, Security and Privacy Issues in Wireless Sensor Networks

for Healthcare Applications, J. Med. Syst. 36 (2012) 93–101. doi:10.1007/s10916-010-9449-4.

[33] P.K. Sahoo, P. Kumar, Efficient Security Mechanisms for mHealth Applications Using Wireless Body Sensor Networks, Sensors. 12 (2012) 12606–12633. doi:10.3390/s120912606.

[34] M. Seyedi, B. Kibret, D.T.H. Lai, M. Faulkner, A survey on intrabody communications for body area network applications, IEEE Trans. Biomed. Eng. 60 (2013) 2067–2079. doi:10.1109/TBME.2013.2254714.

[35] Y. Kim, W.S. Lee, V. Raghunathan, N.K. Jha, A. Raghunathan, Vibration-based secure side channel for medical devices, v: Proc. 52nd Annu. Des. Autom. Conf. - DAC '15, ACM Press, New York, New York, USA, 2015: str. 1–6. doi:10.1145/2744769.2744928.

[36] T. Hayajneh, G. Almashaqbeh, S. Ullah, A. V. Vasilakos, A survey of wireless technologies coexistence in WBAN: analysis and open research issues, Wirel. Networks. 20 (2014) 2165–2199. doi:10.1007/s11276-014-0736-8.

[37] M. Rushanan, A.D. Rubin, D.F. Kune, C.M. Swanson, SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks, v: 2014 IEEE Symp. Secur. Priv., IEEE, 2014: str. 524–539. doi:10.1109/SP.2014.40.

[38] B. Malik, V.R. Singh, A survey of research in WBAN for biomedical and scientific applications, Health Technol. (Berl). 3 (2013) 227–235. doi:10.1007/s12553-013-0056-5.

[39] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, A. Jamalipour, Wireless Body Area Networks: A Survey, IEEE Commun. Surv. Tutorials Commun. Surv. Tutorials. 16 (2014) 1658–1686. doi:10.1109/surv.2013.121313.00064.

[40] V. Mainanwal, M. Gupta, S. Kumar Upadhayay, A Survey on Wireless Body Area Network : Security Technology and its Design Methodology issue, 2nd Int. Conf. Innov. Information,Embedded Commun. Syst. (ICIIECS)2015. (2015) 1–5. doi:10.1109/ICIIECS.2015.7193088.

[41] H. Alemdar, C. Ersoy, Wireless sensor networks for healthcare: A survey, Comput. Networks. 54 (2010) 2688–2710. doi:10.1016/j.comnet.2010.05.003.

[42] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, S. Shamshirband, Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications, Egypt. Informatics J. (2016). doi:10.1016/j.eij.2016.11.001.

[43] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, K.S. Kwak, A Comprehensive Survey of Wireless Body Area Networks, J. Med. Syst. 36 (2012) 1065–1094. doi:10.1007/s10916-010-9571-3.

[44] R. Negra, I. Jemili, A. Belghith, Wireless Body Area Networks: Applications and Technologies, Procedia Comput. Sci. 83 (2016) 1274–1281. doi:10.1016/j.procs.2016.04.266.

[45] S. Wang, R. Bie, F. Zhao, N. Zhang, X. Cheng, H.-A. Choi, Security in wearable communications, IEEE Netw. 30 (2016) 61–67. doi:10.1109/MNET.2016.7579028.

[46] S. Sharma, M.M. Tripathi, V.M. Mishra, Survey paper on sensors for body area network in health care, v: 2017 Int. Conf. Emerg. Trends Comput. Commun. Technol., IEEE, 2017: str. 1–6. doi:10.1109/ICETCCT.2017.8280299.

[47] I. Ha, Technologies and Research Trends in Wireless Body Area Networks for Healthcare: A Systematic Literature Review, Int. J. Distrib. Sens. Networks. 2015 (2015)

1–14. doi:10.1155/2015/573538.

[48] B.-S. Kim, K. Kim, K.-I. Kim, A Survey on Mobility Support in Wireless Body Area Networks, Sensors. 17 (2017) 797. doi:10.3390/s17040797.

[49] A. Mosenia, S. Sur-Kolay, A. Raghunathan, N. Jha, Wearable Medical Sensor-based System Design: A Survey, IEEE Trans. Multi-Scale Comput. Syst. (2017) 1–1. doi:10.1109/TMSCS.2017.2675888.

[50] R.A. Khan, A.-S.K. Pathan, The state-of-the-art wireless body area sensor networks: A survey, Int. J. Distrib. Sens. Networks. 14 (2018) 155014771876899. doi:10.1177/1550147718768994.

[51] B. Latré, B. Braem, I. Moerman, C. Blondia, P. Demeester, A survey on wireless body area networks, Wirel. Networks. 17 (2011) 1–18. doi:10.1007/s11276-010-0252-4.

[52] G. V Crosby, T. Ghosh, R. Murimi, C. a Chin, Wireless Body Area Networks for Healthcare : A Survey, Int. J. Ad hoc, Sens. Ubiquitous Comput. 3 (2012).

[53] S.N. Ramli, R. Ahmad, Surveying the Wireless Body Area Network in the realm of wireless communication, 2011 7th Int. Conf. Inf. Assur. Secur. (2011) 58–61. doi:10.1109/ISIAS.2011.6122845.

[54] D.B. Smith, D. Miniutti, T.A. Lamahewa, L.W. Hanlen, Propagation models for body-area networks: A survey and new outlook, IEEE Antennas Propag. Mag. (2013). doi:10.1109/MAP.2013.6735479.

[55] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, R. Verdone, A Survey on Wireless Body Area Networks: Technologies and Design Challenges, IEEE Commun. Surv. Tutorials. PP (2014) 1–23. doi:10.1109/SURV.2014.012214.00007.

[56] B. Ovilla-Martinez, A. Diaz-Perez, J.J. Garza-Saldana, Key establishment protocol for a patient monitoring system based on PUF and PKG, 2013 10th Int. Conf. Expo Emerg. Technol. a Smarter World. (2013) 1–6. doi:10.1109/CEWIT.2013.6713752.

[57] L. Hughes, X. Wang, T. Chen, A Review of Protocol Implementations and Energy Efficient Cross-Layer Design for Wireless Body Area Networks, Sensors. 12 (2012) 14730–14773. doi:10.3390/s121114730.

[58] M. Simec, I. Mica, J. Kakalek, R. Burget, Bandwidth Efficiency of Wireless Networks of WPAN, WLAN, WMAN and WWAN, Wirel. Networks. (2007) 1–15. http://www.elektrorevue.cz/en/articles/analogue-technics/0/bandwidth-efficiency-of-wireless-networks-of-wpan--wlan--wman-and-wwan-1/ (dostopano 21. november 2018.).

[59] A.J. Menezes, P.C. Van Oorschot, S.A. Vanstone, Handbook of applied cryptography, 1 edition, CRC Press, 1996.

[60] S. Bao, C.Y. Poon Carmen, L. Shen, Y. Zhang, Authenticated symmetric-key establishment for medical body sensor networks, J. Electron. 24 (2007) 421–427. doi:10.1007/s11767-006-0152-z.

[61] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM. 21 (1978) 120–126. doi:10.1145/359340.359342.

[62] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory. 31 (1985) 469–472. doi:10.1109/TIT.1985.1057074.

[63] O. Sarv, Comparing ECC vs RSA, (2018). https://www.linkedin.com/pulse/comparing-

ecc-vs-rsa-ott-sarv (dostopano 1. april 2019.).

[64] D. McGrew, K. Igoe, M. Salter, Fundamental Elliptic Curve Cryptography Algorithms, (2011). https://tools.ietf.org/html/rfc6090 (dostopano 8. marec 2019.).

[65] P.K. Dhillon, S. Kalra, Elliptic curve cryptography for real time embedded systems in IoT networks, v: 2016 5th Int. Conf. Wirel. Networks Embed. Syst., IEEE, 2016: str. 1–6. doi:10.1109/WECON.2016.7993462.

[66] National Security Agency, The Case for Elliptic Curve Cryptography, (b. d.). https://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml (dostopano 7. februar 2018.).

[67] I. Ahmed, Y. Ye, S. Bhattacharya, N. Asokan, G. Jacucci, P. Nurmi, S. Tarkoma, Checksum Gestures: Continuous Gestures as an Out-of-Band Channel for Secure Pairing, v: Proc. 2015 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. - UbiComp '15, ACM Press, New York, New York, USA, 2015: str. 391–401. doi:10.1145/2750858.2807521.

[68] M. Guennoun, M. Zandi, K. El-Khatib, On the Use of Biometrics to Secure Wireless Biosensor Networks, 2008 3rd Int. Conf. Inf. Commun. Technol. From Theory to Appl. (2008) 1–5. doi:10.1109/ICTTA.2008.4530273.

[69] S. Cherukuri, K.K. Venkatasubramanian, S.K.S. Gupta, Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body, v: 2003 Int. Conf. Parallel Process. Work. 2003. Proceedings., IEEE Comput. Soc, 2003: str. 432–439. doi:10.1109/ICPPW.2003.1240399.

[70] K.C. Barr, K. Asanović, Energy-aware lossless data compression, ACM Trans. Comput. Syst. 24 (2006) 250–291. doi:10.1145/1151690.1151692.

[71] S.M.K.-R. Raazi, H. Lee, S. Lee, Y.-K. Lee, BARI: A Distributed Key Management Approach for Wireless Body Area Networks, 2009 Int. Conf. Comput. Intell. Secur. (2009) 324–329. doi:10.1109/CIS.2009.186.

[72] G. Selimis, L. Huang, F. Massé, I. Tsekoura, M. Ashouei, F. Catthoor, J. Huisken, J. Stuyt, G. Dolmans, J. Penders, H. De Groot, A lightweight security scheme for wireless body area networks: Design, energy evaluation and proposed microprocessor design, J. Med. Syst. 35 (2011) 1289–1298. doi:10.1007/s10916-011-9669-2.

[73] M. a. Simplício, P.S.L.M. Barreto, C.B. Margi, T.C.M.B. Carvalho, A survey on key management mechanisms for distributed Wireless Sensor Networks, Comput. Networks. 54 (2010) 2591–2612. doi:10.1016/j.comnet.2010.04.010.

[74] L. Shi, J. Yuan, S. Yu, M. Li, MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks, Internet Things Journal, IEEE. 2 (2015) 52–62. doi:10.1109/JIOT.2015.2391113.

[75] J. Liu, Q. Li, R. Yan, R. Sun, Efficient authenticated key exchange protocols for wireless body area networks, EURASIP J. Wirel. Commun. Netw. 2015 (2015) 188. doi:10.1186/s13638-015-0406-2.

[76] E. Alasaarela, Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system, Int. Conf. Inf. Netw. 2014. (2014) 453–457. doi:10.1109/ICOIN.2014.6799723.

[77] L. Yao, B. Liu, K. Yao, G. Wu, J. Wang, An ECG-based signal key establishment protocol in body area networks, Proc. - Symp. Work. Ubiquitous, Auton. Trust. Comput. Conjunction with UIC 2010 ATC 2010 Conf. UIC-ATC 2010. (2010) 233–238. doi:10.1109/UIC-ATC.2010.7.

[78] Xiangxue Li, Weidong Qiu, Dong Zheng, Kefei Chen, Jianhua Li, Anonymity Enhancement on Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards, IEEE Trans. Ind. Electron. 57 (2010) 793–800. doi:10.1109/TIE.2009.2028351.

[79] D. Hughes, V. Shmatikov, Information hiding, anonymity and privacy: a modular approach, J. Comput. Secur. 12 (2004) 3–36. doi:10.3233/JCS-2004-12102.

[80] N.U. Amin, M. Asad, S.A. Chaudhry, An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem, Networking, Sens. Control (ICNSC), 2012 9th IEEE Int. Conf. (2012) 118–121. doi:10.1109/ICNSC.2012.6204902.

[81] C. Boyd, A. Mathuria, Protocols for Authentication and Key Establishment, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003. doi:10.1007/978-3-662-09527-0.

[82] C. Cremers, M. Feltz, Beyond eCK: Perfect Forward Secrecy under Actor Compromise and Ephemeral-Key Reveal, v: Springer, Berlin, Heidelberg, 2012: str. 734–751. doi:10.1007/978-3-642-33167-1_42.

[83] H.S. Ng, M.L. Sim, C.M. Tan, Security issues of wireless sensor networks in healthcare applications, BT Technol. J. (2006).

[84] C. Huang, H. Lee, D.H. Lee, A Privacy-Strengthened Scheme for E-Healthcare Monitoring System, J. Med. Syst. 36 (2012) 2959–2971. doi:10.1007/s10916-011-9774-2.

[85] W. Drira, E. Renault, D. Zeghlache, A Hybrid Authentication and Key Establishment Scheme for WBAN, 2012 IEEE 11th Int. Conf. Trust. Secur. Priv. Comput. Commun. (2012) 78–83. doi:10.1109/TrustCom.2012.31.

[86] C.C. Tan, H. Wang, S. Zhong, Q. Li, IBE-lite: A lightweight identity-based cryptography for body sensor networks, IEEE Trans. Inf. Technol. Biomed. 13 (2009) 926–932. doi:10.1109/TITB.2009.2033055.

[87] L. Ma, Y. Ge, Y. Zhu, TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks, Wirel. Pers. Commun. 77 (2014) 1077–1090. doi:10.1007/s11277-013-1555-4.

[88] O. García-Morchón, D. Gómez-Pérez, J. Gutiérrez, R. Rietman, B. Schoenmakers, L. Tolhuizen, HIMMO: A Lightweight Collusion-Resistant Key Predistribution Scheme, (b. d.).

[89] K. Chalkias, F. Mpaldimtsi, D. Hristu-Varsakelis, G. Stephanides, On the Key-Compromise Impersonation Vulnerability of One-Pass Key Establishment Protocols, SECRYPT. (2007) 222–228.

[90] X. Li, M.H. Ibrahim, S. Kumari, A.K. Sangaiah, V. Gupta, K.-K.R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, Comput. Networks. 129 (2017) 429–443. doi:10.1016/J.COMNET.2017.03.013.

[91] V.P. Singh, S. Jain, J. Singhai, Hello Flood Attack and its Countermeasures in Wireless Sensor Networks, Int. J. Comput. Sci. 7 (2010) 23. http://www.ijcsi.org/papers/IJCSI-Vol-7-Issue-3-No--11.pdf#page=37.

[92] J.R. Douceur, The Sybil Attack, v: Proc. 1st Int. Work. Peer-to-Peer Syst., Springer, 2002.

[93] H. Yih-Chun, A. Perrig, D. B. Johnson, Wormhole attacks in wireless networks, IEEE J. Sel. Areas Commun. 24 (2006) 370–380. doi:10.1109/JSAC.2005.861394.

[94] M. Kompara, M. Hölbl, Survey on security in intra-body area network communication,

Ad Hoc Networks. 70 (2018) 23–43. doi:10.1016/J.ADHOC.2017.11.006.

[95] K.S.K. Jingwei Liu, Hybrid security mechanisms for wireless body area networks, 2010 Second Int. Conf. Ubiquitous Futur. Networks. (2010) 98–103. doi:10.1109/ICUFN.2010.5547221.

[96] M.R. Kanjee, K. Divi, H. Liu, A Two-Tiered Authentication and Encryption Scheme in Secure Healthcare Sensor Networks, v: 2010 7th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks, 2010: str. 1–3. doi:10.1109/SECON.2010.5508215.

[97] Z. Mehmood, S.A. Ch, W. Nasar, A. Ghani, An efficient key agreement with rekeying for secured body sensor networks, 2012 Second Int. Conf. Digit. Inf. Process. Commun. (2012) 164–167. doi:10.1109/ICDIPC.2012.6257295.

[98] A. Sudarsono, M.U.H. Al Rasyid, H. Hermawan, An implementation of secure wireless sensor network for e-healthcare system, 2014 Int. Conf. Comput. Control. Informatics Its Appl. (2014) 69–74. doi:10.1109/IC3INA.2014.7042603.

[99] M. Barua, M.S. Alam, X. Liang, X. Shen, Secure and quality of service assurance scheduling scheme for WBAN with application to eHealth, 2011 IEEE Wirel. Commun. Netw. Conf. WCNC 2011. (2011) 1102–1106. doi:10.1109/WCNC.2011.5779285.

[100] K.M. Sharmilee, R. Mukesh, A. Damodaram, V.S. Bharathi, Secure WBAN using rule-based IDS with biometrics and MAC authentication, 2008 10th IEEE Intl. Conf. e-Health Networking, Appl. Serv. Heal. 2008. (2008) 102–107. doi:10.1109/HEALTH.2008.4600119.

[101] D.J. Malan, M. Welsh, M.D. Smith, A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography, v: 2004 First Annu. IEEE Commun. Soc. Conf. Sens. Ad Hoc Commun. Networks, 2004. IEEE SECON 2004., IEEE, 2004: str. 71–80. doi:10.1109/SAHCN.2004.1381904.

[102] N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, v: M. Joye, J.-J. Quisquater (Ur.), 6th Int. Work. Cambridge, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004. doi:10.1007/b99451.

[103] K. Malasri, L. Wang, Addressing security in medical sensor networks, v: 1st ACM SIGMOBILE Int. Work. Syst. Netw. Support Healthc. Assist. living Environ. ACM, 2007: str. 7–12. doi:10.1145/1248054.1248058.

[104] J.-M. Ho, A versatile suite of strong authenticated key agreement protocols for body area networks, 2012 8th Int. Wirel. Commun. Mob. Comput. Conf. (2012) 683–688. doi:10.1109/IWCMC.2012.6314287.

[105] J. Shen, S. Moh, I. Chung, A Novel Key Management Protocol in Body Area Networks, v: 7th Int. Conf. Netw. Serv., 2011.

[106] J. Shen, H. Tan, S. Moh, I. Chung, Q. Liu, X. Sun, Enhanced secure sensor association and key management in wireless body area networks, J. Commun. Networks. 17 (2015) 453–462. doi:10.1109/JCN.2015.000083.

[107] J. Iqbal, N. Amin, A.I. Umar, Authenticated key agreement and cluster head selection for Wireless Body Area Networks, 2nd Natl. Conf. Inf. Assur. (2013) 113–117. doi:10.1109/NCIA.2013.6725334.

[108] S. Challa, A.K. Das, V. Odelu, N. Kumar, Kumari Saru, M.K. Khan, A. V. Vasilakos, An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks, Comput. Electr. Eng. (2017). doi:10.1016/J.COMPELECENG.2017.08.003.

[109] K.-H. Yeh, A Secure IoT-based Healthcare System with Body Sensor Networks, IEEE Access. 4 (2016) 10288–10299. doi:10.1109/ACCESS.2016.2638038.

[110] S. Möller, T. Newe, S. Lochmann, Prototype of a secure wireless patient monitoring system for the medical community, Sensors Actuators A Phys. 173 (2012) 55–65. doi:10.1016/j.sna.2011.10.016.

[111] X. Huang, Q. Wang, C. Bangdao, A. Markham, R. Jäntti, A.W. Roscoe, Body sensor network key distribution using human interactive channels, v: Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol., 2011. doi:10.1145/2093698.2093841.

[112] C. Rong, H. Cheng, Authenticated Health Monitoring Scheme for Wireless Body Sensor Networks, Proc. 7th Int. Conf. Body Area Networks. (2012) 31–35. doi:10.4108/icst.bodynets.2012.249945.

[113] C.C. Tan, H. Wang, S. Zhong, Q. Li, Body Sensor network security: an identity based cryptography approach, ACM Conf. Wirel. Netw. Secur. (2008) 148–153. doi:10.1145/1352533.1352557.

[114] S. Venkatasubramanian, V. Jothi, Integrated authentication and security check with CDMA modulation technique in physical layer of Wireless Body Area Network, 2012 IEEE Int. Conf. Comput. Intell. Comput. Res. (2012) 1–6. doi:10.1109/ICCIC.2012.6510239.

[115] M. Sarvabhatla, C.S. Vorugunti, An energy efficient mutual authentication scheme for secure data exchange in health-care applications using wireless body sensor network, 2015 7th Int. Conf. Commun. Syst. Networks. (2015) 1–6. doi:10.1109/COMSNETS.2015.7098704.

[116] L. Ming, Y. Shucheng, L. Wenjing, R. Kui, Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks, v: Proc. 29th Conf. Inf. Commun., 2010: str. 1–9. doi:10.1109/INFCOM.2010.5462095.

[117] M. Li, S. Yu, J.D. Guttman, W. Lou, K. Ren, Secure ad hoc trust initialization and key management in wireless body area networks, ACM Trans. Sens. Networks. 9 (2013) 1–35. doi:10.1145/2422966.2422975.

[118] T. Kovačević, T. Perković, M. Čagalj, LIRA: A New Key Deployment Scheme for Wireless Body Area Networks, Software, Telecommun. Comput. Networks (SoftCOM), 2013 21st Int. Conf. (2013).

[119] Q. Wang, A. Markham, Z. Yan, A.W. Roscoe, B. Chen, X. Huang, Human interactive secure key and identity exchange protocols in body sensor networks, IET Inf. Secur. 7 (2013) 30–38. doi:10.1049/iet-ifs.2012.0080.

[120] D.S. Sanchez, H. Baldus, A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks, v: First Int. Conf. Secur. Priv. Emerg. Areas Commun. Networks, IEEE, 2005: str. 277–288. doi:10.1109/SECURECOMM.2005.2.

[121] Y. Ren, V. Oleshchuk, F.Y. Li, S. Sulistyo, FoSBaS: a bi-directional secrecy and collusion resilience key management scheme for BANs, 2012 IEEE Wirel. Commun. Netw. Conf. (2012) 2841–2846. doi:10.1109/WCNC.2012.6214286.

[122] M.R. Abdmeziem, D. Tandjaoui, An end-to-end secure key management protocol for e-health applications, Comput. Electr. Eng. 44 (2015) 184–197. doi:10.1016/j.compeleceng.2015.03.030.

[123] M.H. Ibrahim, S. Kumari, A.K. Das, M. Wazid, V. Odelu, Secure anonymous mutual authentication for star two-tier wireless body area networks, Comput. Methods

Programs Biomed. 135 (2016) 37–50. doi:10.1016/j.cmpb.2016.07.022.

[124] O.G. Morchon, H. Baldus, D.S. Sanchez, Resource-efficient security for medical body sensor networks, Int. Work. Wearable Implant. Body Sens. Networks, 2006. (2006) 4–pp. doi:10.1109/BSN.2006.45.

[125] O.G. Morchon, H. Baldus, Efficient distributed security for wireless medical sensor networks, v: ISSNIP 2008 - Proc. 2008 Int. Conf. Intell. Sensors, Sens. Networks Inf. Process., 2008: str. 249–254. doi:10.1109/ISSNIP.2008.4761995.

[126] B. Lamichhane, S. Mudda, F. Regazzoni, A. Puiatti, LEXCOMM: A low energy, secure and flexible communication protocol for a heterogenous body sensor network, Proc. - IEEE-EMBS Int. Conf. Biomed. Heal. Informatics Glob. Gd. Chall. Heal. Informatics, BHI 2012. 25 (2012) 273–276. doi:10.1109/BHI.2012.6211564.

[127] D. Singelée, B. Latré, B. Braem, M. Peeters, M. De Soete, P. De Cleyn, B. Preneel, I. Moerman, C. Blondia, A Secure Cross-Layer Protocol for Multi-hop Wireless Body Area Networks, Ad-hoc, Mob. Wirel. Networks. (2008) 94–107. doi:10.1007/978-3-540-85209-4_8.

[128] K.K. Venkatasubramanian, S.K.S. Gupta, Physiological value-based efficient usable security solutions for body sensor networks, ACM Trans. Sens. Networks. 6 (2010) 1–36. doi:10.1145/1777406.1777410.

[129] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, S. Member, PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks, IEEE Trans. Inf. Technol. Biomed. 14 (2010) 60–68.

[130] F.M. Bui, D. Hatzinakos, Resource allocation strategies for secure and efficient communications in biometrics-based body sensor networks, v: Biometrics Symp., 2007.

[131] H. Wang, H. Fang, L. Xing, M. Chen, An Integrated Biometric-Based Security Framework Using Wavelet-Domain HMM in Wireless Body Area Networks (WBAN), 2011 IEEE Int. Conf. Commun. (2011) 1–5. doi:10.1109/icc.2011.5962757.

[132] S.-D. Bao, F. Miao, Y. Li, Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security, IET Inf. Secur. 7 (2013) 87–96. doi:10.1049/iet-ifs.2012.0104.

[133] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, D. Chen, OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks, IEEE Int. Conf. Comput. Commun. (2013) 2274–2282. doi:10.1109/INFCOM.2013.6567031.

[134] N. Jamali, L.C. Fourati, SKEP : a Secret Key Exchange Protocol using physiological signals in wireless body area networks, 2015 Int. Conf. Wirel. Networks Mob. Commun. (2015).

[135] N. Jammali, L.C. Fourati, PFKA: A Physiological Feature based Key Agreement for Wireless Body Area Network, v: 2015 Int. Conf. Wirel. Networks Mob. Commun., 2015.

[136] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, EKG-based Key Agreement in Body Sensor Networks, v: IEEE Int. Conf. Comput. Commun., 2008.

[137] A. Ali, S. Irum, F. Kausar, F.A. Khan, A cluster-based key agreement scheme using keyed hashing for Body Area Networks, v: Multimed. Tools Appl., 2013: str. 201–214. doi:10.1007/s11042-011-0791-4.

[138] F. Xu, Z. Qin, C.C. Tan, B. Wang, Q. Li, IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian, v: IEEE Int. Conf. Comput. Commun., 2011: str. 1862–1870.

[139] A. Ali, F.A. Khan, A broadcast-based key agreement scheme using set reconciliation for wireless body area networks, J. Med. Syst. 38 (2014) 33. doi:10.1007/s10916-014-0033-1.

[140] F.M. Bui, D. Hatzinakos, Biometric Methods for Secure Communications in Body Sensor Networks: Resource-Efficient Key Management and Signal-Level Data Scrambling, EURASIP J. Adv. Signal Process. 2008 (2008). doi:10.1155/2008/529879.

[141] F. Miao, L. Jiang, Y. Li, Y.-T. Zhang, A Novel Biometrics Based Security Solution for Body Sensor Networks, 2009 2nd Int. Conf. Biomed. Eng. Informatics. (2009) 1–5. doi:10.1109/BMEI.2009.5304950.

[142] F. Miao, L. Jiang, Y. Li, Y.-T. Zhang, Biometrics based novel key distribution solution for body sensor networks., Conf. Proc. IEEE Eng. Med. Biol. Soc. 2009 (2009) 2458–61. doi:10.1109/IEMBS.2009.5334698.

[143] Q. Huang, C. Guo, Efficient Key Cryptography Based on Body Area Networks, v: Proc. 2011 IEEE Int. Conf. Cyber Technol. Autom. Control. Intell. Syst., Kunming, 2011: str. 171–174.

[144] W. Wang, H. Wang, M. Hempel, Secure Stochastic ECG Signals Based on Gaussian Mixture Model for-Healthcare Systems, IEEE Syst. J. 5 (2011) 564–573. doi:10.1109/JSYST.2011.2165597.

[145] Z. Zhang, H. Wang, A. V. Vasilakos, H. Fang, ECG-cryptography and authentication in body area networks, IEEE Trans. Inf. Technol. Biomed. 16 (2012) 1070–1078. doi:10.1109/TITB.2012.2206115.

[146] E.K. Zaghouani, A. Jemai, A. Benzina, R. Attia, ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN, v: 23rd Eur. Signal Process. Conf., 2015: str. 81–85.

[147] K.K. Venkatasubramanian, A. Banerjee, S.K.S. Gupta, Plethysmogram-based secure inter-sensor communication in body area networks, Proc. - IEEE Mil. Commun. Conf. MILCOM. (2008). doi:10.1109/MILCOM.2008.4753199.

[148] M.R. Kanjee, K. Divi, H. Liu, A Physiological Authentication Scheme in Secure Healthcare Sensor Networks, v: 7th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks, 2010: str. 1–3.

[149] S. Saleem, S. Ullah, K.S. Kwak, Towards security issues and solutions in Wireless Body Area Networks, Networked Comput. (INC), 2010 6th Int. Conf. (2010) 1–4. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5484803.

[150] S.-D. Bao, Y.-T. Zhang, L.-F. Shen, A design proposal of security architecture for medical body sensor networks, v: Int. Work. Wearable Implant. Body Sens. Networks, 2006: str. 84–87. doi:10.1109/BSN.2006.2.

[151] J. Zhou, Z. Cao, X. Dong, BDK: Secure and Efficient Biometric Based Deterministic Key Agreement in Wireless Body Area Networks, Proc. 8th Int. Conf. Body Area Networks. 1 (2013) 488–494. doi:10.4108/icst.bodynets.2013.253731.

[152] Y. Lu, S.-D. Bao, Efficient fuzzy vault application in node recognition for securing body sensor networks, IEEE Int. Conf. Commun. (2014) 3648–3651. doi:10.1109/ICC.2014.6883888.

[153] F. Miao, S.-D. Bao, Y. Li, A Modified Fuzzy Vault Scheme for Biometrics-Based Body Sensor Networks Security, 2010 IEEE Glob. Telecommun. Conf. GLOBECOM 2010. (2010) 1–5. doi:10.1109/GLOCOM.2010.5683998.

[154] C.Z. Cao, C.G. He, S. Di Bao, Y. Li, Improvement of fuzzy vault scheme for securing key distribution in body sensor network, Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS. (2011) 3563–3567. doi:10.1109/IEMBS.2011.6090594.

[155] R.T. Rajasekaran, V. Manjula, V. Kishore, T.M. Sridhar, C. Jayakumar, An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Networks, v: Int. Conf. Adv. Comput. Commun. Informatics, 2012. doi:10.1145/2345396.2345579.

[156] A. Juels, M. Sudan, A fuzzy vault scheme, Des. Codes Cryptogr. 38 (2006) 237–257. doi:10.1007/s10623-005-6343-z.

[157] K. Cho, D. Lee, Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks, Lect. Notes Comput. Sci. 7115 (2012) 203–218. doi:10.1007/978-3-642-27890-7_17.

[158] A. Ali, F.A. Khan, An Improved EKG-Based Key Agreement Scheme for Body Area Networks, v: 4th Int. Conf. Inf. Secur. Assur., Miyazaki, Japan, 2010: str. 298–308. http://www.springerlink.com/index/10.1007/978-3-642-13365-7 (dostopano 11. maj 2017.).

[159] J. Shi, K.-Y. Lam, M. Gu, M. Li, S.-L. Chung, Towards Energy-Efficient Secure Communications Using Biometric Key Distribution in Wireless Biomedical Healthcare Networks, v: 2nd Int. Conf. Biomed. Eng. Informatics, 2009: str. 1–5. doi:10.1109/BMEI.2009.5304940.

[160] A. Ali, F.A. Khan, Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications, EURASIP J. Wirel. Commun. Netw. (2013) 1–19. doi:10.1186/1687-1499-2013-216.

[161] W. Wang, C. Science, K. Hua, M. Hempel, E. Engineering, D. Peng, H. Sharif, H. Chen, A Stochastic Biometric Authentication Scheme using Uniformed GMM in Wireless Body Area, v: 21st Int. Symp. Pers. Indoor Mob. Radio Commun., IEEE, Instanbul, 2010: str. 1620–1624.

[162] G. Revadigar, C. Javali, H.J. Asghar, K.B. Rasmussen, S. Jha, Mobility Independent Secret Key Generation for Wearable Health-care Devices, v: Proc. 10th EAI Int. Conf. Body Area Networks, ICST, 2015: str. 294–300. doi:10.4108/eai.28-9-2015.2261446.

[163] S.T. Ali, V. Sivaraman, D. Ostry, Zero reconciliation secret key generation for body-worn health monitoring devices, Proc. fifth ACM Conf. Secur. Priv. Wirel. Mob. Networks. (2012) 39–50. doi:10.1145/2185448.2185455.

[164] L.W. Hanlen, D. Smith, J. (Andrew) Zhang, D. Lewis, Key-sharing via channel randomness in narrowband body area networks: Is everyday movement sufficient?, v: Proc. 4th Int. ICST Conf. Body Area Networks, ICST, 2009: str. 17. doi:10.4108/ICST.BODYNETS2009.5941.

[165] S.T. Ali, V. Sivaraman, D. Ostry, Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks, v: 2010 IEEE/IFIP Int. Conf. Embed. Ubiquitous Comput., IEEE, 2010: str. 644–650. doi:10.1109/EUC.2010.103.

[166] L. Yao, T.A. Ali, V. Sivaraman, D. Ostry, Improving secret key generation performance for on-body devices, v: Proc. 6th Int. Conf. Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2011. http://dl.acm.org/citation.cfm?id=2318782&CFID=719860224&CFTOKEN=99013021 (dostopano 10. marec 2017.).

[167] G.R. Tsouri, J. Wilczewski, Reliable symmetric key generation for body area networks using wireless physical layer security in the presence of an on-body eavesdropper, v:

Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol. - ISABEL '11, ACM Press, New York, New York, USA, 2011: str. 1–6. doi:10.1145/2093698.2093851.

[168] Y. Wu, Y. Sun, L. Zhan, Y. Ji, Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network, Int. J. Distrib. Sens. Networks. (2013). doi:10.1155/2013/912873.

[169] Z. Zhang, H. Wang, A. V Vasilakos, Channel Information based Cryptography and Authentication in Wireless Body Area Networks, v: 8th Int. Conf. Body Area Networks, 2013: str. 2–5.

[170] L. Shi, J. Yuan, S. Yu, M. Li, ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks, v: Sixth ACM Conf. Secur. Priv. Wirel. Mob. networks, 2013. doi:10.1109/JIOT.2015.2391113.

[171] R. Dautov, G.R. Tsouri, Securing while Sampling in Wireless Body Area Networks with Application to Electrocardiography, IEEE J. Biomed. Heal. informatics. PP (2014) 1. doi:10.1109/JBHI.2014.2366125.

[172] C. Javali, G. Revadigar, L. Libman, S. Jha, SeAK: Secure Authentication and Key Generation Protocol Based on Dual Antennas for Wireless Body Area Networks, v: Springer, Cham, 2014: str. 74–89. doi:10.1007/978-3-319-13066-8_5.

[173] G. Revadigar, C. Javali, W. Hu, S. Jha, DLINK: Dual link based radio frequency fingerprinting for wearable devices, v: 2015 IEEE 40th Conf. Local Comput. Networks, IEEE, 2015: str. 329–337. doi:10.1109/LCN.2015.7366327.

[174] L. Yao, S.T. Ali, V. Sivaraman, D. Ostry, Decorrelating secret bit extraction via channel hopping in body area networks, v: 2012 IEEE 23rd Int. Symp. Pers. Indoor Mob. Radio Commun. -, IEEE, 2012: str. 1454–1459. doi:10.1109/PIMRC.2012.6362577.

[175] G. Revadigar, C. Javali, H.J. Asghar, K.B. Rasmussen, S. Jha, iARC: Secret Key Generation for Resource Constrained Devices by Inducing Artificial Randomness in the Channel, v: Proc. 10th ACM Symp. Information, Comput. Commun. Secur. - ASIA CCS '15, ACM Press, New York, New York, USA, 2015: str. 669–669. doi:10.1145/2714576.2714644.

[176] C. Javali, G. Revadigar, M. Ding, S. Jha, Secret Key Generation by Virtual Link Estimation, v: Proc. 10th EAI Int. Conf. Body Area Networks, ICST, 2015: str. 301–307. doi:10.4108/eai.28-9-2015.2261448.

[177] G. Revadigar, C. Javali, H.J. Asghar, K.B. Rasmussen, S. Jha, Secret Key Generation for Body-worn Devices by Inducing Artificial Randomness in the Channel, 2015. http://www.cse.unsw.edu.au/~chitraj/assets/papers/UNSW_CSE_TR006_Javali.pdf (dostopano 10. april 2017.).

[178] J. Lester, J. Lester, B. Hannaford, G. Borriello, Are You with Me?" – using accelerometers to determine if two devices are carried by the same person, Proc. Second Int. Conf. PERVASIVE Comput. (PERVASIVE 2004. 3001 (2004) 33--50. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.75.2328 (dostopano 24. marec 2017.).

[179] D. Bichler, G. Stromberg, M. Huemer, M. Löw, Key Generation Based on Acceleration Data of Shaking Processes, v: UbiComp 2007 Ubiquitous Comput., Springer Berlin Heidelberg, Berlin, Heidelberg, 2007: str. 304–317. doi:10.1007/978-3-540-74853-3_18.

[180] R. Mayrhofer, H. Gellersen, Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices, IEEE Trans. Mob. Comput. 8 (2009) 792–806. doi:10.1109/TMC.2009.51.

[181] W. Xu, G. Revadigar, C. Luo, N. Bergmann, W. Hu, Walkie-Talkie: Motion-Assisted

Automatic Key Generation for Secure On-Body Device Communication, v: 2016 15th ACM/IEEE Int. Conf. Inf. Process. Sens. Networks, IEEE, 2016: str. 1–12. doi:10.1109/IPSN.2016.7460726.

[182] W. Xu, C. Javali, G. Revadigar, C. Luo, N. Bergmann, W. Hu, Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices, ACM Trans. Sens. Networks. 13 (2017) 1–27. doi:10.1145/3023954.

[183] G. Revadigar, C. Javali, W. Xu, W. Hu, S. Jha, Secure key generation and distribution protocol for wearable devices, v: 2016 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work., IEEE, 2016: str. 1–4. doi:10.1109/PERCOMW.2016.7457058.

[184] Q. Quach, N. Nguyen, T. Dinh, Secure Authentication for Mobile Devices Based on Acoustic Background Fingerprint, v: Springer, Cham, 2014: str. 375–387. doi:10.1007/978-3-319-02741-8_32.

[185] D. Oberoi, Wing Yan Sou, Yin Yi Lui, R. Fisher, L. Dinca, G.P. Hancke, Wearable security: Key derivation for Body Area sensor Networks based on host movement, v: 2016 IEEE 25th Int. Symp. Ind. Electron., IEEE, 2016: str. 1116–1121. doi:10.1109/ISIE.2016.7745050.

[186] A. Juels, M. Wattenberg, A Fuzzy Commitment Scheme, CCS '99 Proc. 6th ACM Conf. Comput. Commun. Secur. (1999) 28–36. doi:10.1145/319709.319714.

[187] K.K. Venkatasubramanian, S.K.S. Gupta, Security for Pervasive Health Monitoring Sensor Applications, Fourth Int. Conf. Intell. Sens. Inf. Process. (2006) 197–202. doi:10.1109/ICISIP.2006.4286096.

[188] H. Zhao, J. Qin, J. Hu, An Energy Efficient Key Management Scheme for Body Sensor Networks, IEEE Trans. Parallel Distrib. Syst. 24 (2013) 2202–2210.

[189] A.S. Sangari, J.M.L. Manickam, Public Key Cryptosystem Based Security in Wireless Body Area Network, v: Int. Conf. Circuit, Power Comput. Technol., 2014: str. 1609–1612.

[190] G.H. Zhang, C.C.Y. Poon, Y. Li, Y.T. Zhang, A biometric method to secure telemedicine systems., Conf. Proc. IEEE Eng. Med. Biol. Soc. 2009 (2009) 701–4. doi:10.1109/IEMBS.2009.5332470.

[191] S.M.K.-R. Raazi, S. Lee, Y.-K. Lee, A Novel Architecture for Efficient Key Management in Humanware Applications, Fifth Int. Jt. Conf. INC, IMS IDC. (2009) 1918–1922. doi:10.1109/NCM.2009.335.

[192] K.-R.R.S. Muhammad, H. Lee, S. Lee, Y.-K. Lee, BARI+: a biometric based distributed key management approach for wireless body area networks., Sensors. 10 (2010) 3911–33. doi:10.3390/s100403911.

[193] A. Alsadhan, N. Khan, An LBP Based Key Management for Secure Wireless Body Area Network (WBAN), 14th ACIS Int. Conf. Softw. Eng. Artif. Intell. Netw. Parallel/Distributed Comput. (2013) 85–88. doi:10.1109/SNPD.2013.32.

[194] M.M. Mana, SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network), Int. J. Adv. Sci. Technol. 12 (2009) 45–60. http://www.earticle.net/Article.aspx?sn=147319.

[195] M. Mana, M. Feham, B. Bensaber, Trust Key Management Scheme for Wireless Body Area Networks., Int. J. Netw. Secur. 12 (2011) 71–79. http://ijns.femto.com.tw/contents/ijns-v12-n1/ijns-2011-v12-n1-p71-79.pdf.

[196] S. Irum, A. Ali, F.A. Khan, H. Abbas, A hybrid security mechanism for intra-wban and inter-WBAN communications, Int. J. Distrib. Sens. Networks. 2013 (2013).

doi:10.1155/2013/842608.

[197] D. He, C. Chen, S. Chan, J. Bu, P. Zhang, Secure and lightweight network admission and transmission protocol for body sensor networks, IEEE J. Biomed. Heal. Informatics. 17 (2013) 664–674. doi:10.1109/JBHI.2012.2235180.

[198] L. Yao, B. Liu, G. Wu, K. Yao, J. Wang, A biometric key establishment protocol for body area networks, Int. J. Distrib. Sens. Networks. 2011 (2011). doi:10.1155/2011/282986.

[199] M. Rostami, A. Juels, F. Koushanfar, M. Rostami, A. Juels, F. Koushanfar, Heart-to-Heart (H2H): Authentication for Implanted Medical Devices, v: Proc. 2013 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '13, ACM Press, New York, New York, USA, 2013: str. 1099–1112. doi:10.1145/2508859.2516658.

[200] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Trans. Comput. Syst. 8 (1990) 18–36. doi:10.1145/77648.77649.

[201] P.F. Syverson Code, P.C. Van Oorschot, A Unified Cryptographic Protocol Logic, 1996. NRL CHACS Report 5540-227.

[202] AVISPA: Automated Validation of Internet Security Protocols and Applications, (b. d.). http://www.avispa-project.org/ (dostopano 18. oktober 2018.).

[203] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, (2010). doi:10.6028/NIST.SP.800-22r1a.

[204] G.K. Ragesh, K. Baskaran, CRYPE: towards cryptographically enforced and privacy enhanced WBANs, Proc. First Int. Conf. Secur. Internet Things - Secur. '12. (2012) 204–209. doi:10.1145/2490428.2490457.

[205] M. Kompara, S. Kumari, M. Hölbl, Analysis and improvement of a secure key management protocol for e-health applications, Comput. Electr. Eng. (2019). doi:10.1016/j.compeleceng.2018.11.007.

[206] M. Dworkin, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, NIST Spec. Publ. (b. d.) 800–38. doi:10.6028/NIST.SP.800-38c.

[207] M.H. Behringer, End-to-End Security, Internet Protoc. J. 12 (2009). https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-45/123-security.html.

[208] E. Barker, Recommendation for Key Management, NIST Special Publication 800-57 Part 1 Revision 4, b. d. doi:10.6028/NIST.SP.800-57pt1r4.

[209] J.-P. Kaps, B. Sunar, Energy Comparison of AES and SHA-1 for Ubiquitous Computing, v: Int. Conf. Embed. Ubiquitous Comput., 2006: str. 372–381. doi:10.1007/11807964_38.

[210] M. Passing, F. Dressler, Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes, v: 2006 IEEE Int. Conf. Mob. Ad Hoc Sens. Sysetems, IEEE, 2006: str. 882–887. doi:10.1109/MOBHOC.2006.278669.

[211] G. de Meulenaer, F. Gosset, F.-X. Standaert, O. Pereira, On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks, v: 2008 IEEE Int. Conf. Wirel. Mob. Comput. Netw. Commun., IEEE, 2008: str. 580–585. doi:10.1109/WiMob.2008.16.

[212] M. Kompara, S.H. Islam, M. Hölbl, A robust and efficient mutual authentication and key

agreement scheme with untraceability for WBANs, Comput. Networks. (2019). doi:10.1016/j.comnet.2018.11.016.

[213] L. Mearian, CW@50: Data storage comes into its own, (2017). https://www.computerworld.com/article/3182140/cw-50-the-data-storage-industry-comes-into-its-own.html (dostopano 3. april 2019.).

[214] STM32F103VE - Mainstream Performance line, ARM Cortex-M3 MCU with 512 Kbytes Flash, 72 MHz CPU, motor control, USB and CAN - STMicroelectronics, (b. d.). http://www.st.com/en/microcontrollers/stm32f103ve.html (dostopano 23. april 2018.).